

Svjetsko tržište kriptovaluta

Skrbin, Marcela-Maria

Master's thesis / Diplomski rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Economics and Business / Sveučilište u Zagrebu, Ekonomski fakultet**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:148:187159>

Rights / Prava: [In copyright](#)/[Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-07-14**



Repository / Repozitorij:

[REPEFZG - Digital Repository - Faculty of Economics & Business Zagreb](#)



Sveučilište u Zagrebu
Ekonomski fakultet
Integrirani preddiplomski i diplomski sveučilišni
studij Poslovna ekonomija, smjer Financije

SVJETSKO TRŽIŠTE KRIPTOVALUTA

Diplomski rad

Marcela-Maria Skrbín

Zagreb, rujan 2021.

Sveučilište u Zagrebu
Ekonomski fakultet
Integrirani preddiplomski i diplomski sveučilišni
studij Poslovna ekonomija, smjer Financije

SVJETSKO TRŽIŠTE KRIPTOVALUTA
WORLD CRYPTOCURRENCIES MARKET

Diplomski rad

Student: Marcela-Maria Skrbín

JMBAG studenta: 0067539177

Mentor: Prof. dr. sc. Marijana

Ivanov

Zagreb, rujan 2021.

SAŽETAK

Cilj ovoga rada jest analizirati međusobnu interakciju tradicionalog tržišta i kriptovaluta. Preciznije, kriptovalutama će se pristupiti s tehnološkog, ekonomskog i pravnog aspekta kako bi se utvrdio utjecaj, odnosno posljedice koje su kriptovalute unijele ulaskom na tržište. Kriptovalute novi su oblik digitalnog novca, odnosno digitalne imovine, koji nije vezan za centralne banke, već nastaje doprinosom rudara kriptozajednici. One nastaju na temelju složenih kriptografskih algoritama čije su tehnike bazirane na blockchain tehnologiji. Budući da je upravo blockchain tehnologija sastavni dio danas aktualne četvrte industrijske revolucije, kriptovalute utjecat će na sve aspekte društva: ekonomske, političke, društvene i kulturološke. Njihove glavne prednosti leže u anonimnosti, decentralizaciji te manjim troškovima elektroničkih transakcija. S druge strane, ta ista „labava“ regulacija može olakšati aktivnosti crnog tržišta te izbjegavanje poreza. Jedna od mana koja se također pripisuje kriptovalutama jest njihova iznimna volatilnost. Ona se, međutim, pokušava reducirati razvojem brojnih matematičkih modela koji u kombinaciji s tehničkom analizom mogu pomoći u predviđanju kretanja cijena kriptovaluta s većom točnošću. Svjetska se ekonomija konstantno mijenja, a kriptovalute mogle bi s vremenom postati dio elektroničke štednje. Općenito, tržište kriptovaluta aktivno raste, kao i broj njihovih ulagača, pojavljuju se nove tvrtke i infrastrukturni projekti povezani s njima, što se može vidjeti na svjetskoj razini, ali i u malim otvorenim gospodarstvima kao što je Republika Hrvatska čije tvrtke nimalo ne zaostaju što se tiče inovacija na području kriptotehnologije.

Ključne riječi: kriptovalute, rudarenje, kriptoinovacije, regulacija

SUMMARY

The aim of this paper is to analyze the interaction between the traditional market and cryptocurrencies. More precisely, cryptocurrencies will be approached from a technological, economic and legal aspect in order to determine the impact, i.e. the consequences that cryptocurrencies have brought upon entering the market. Cryptocurrencies are a new form of digital money, i.e. digital assets, which is not tied to central banks, but is created by the contribution of miners to the crypto community. They are created on the basis of complex cryptographic algorithms whose techniques are based on blockchain technology. Since blockchain technology is an integral part of the current fourth industrial revolution, cryptocurrencies will affect all aspects of society: economical, political, social and cultural. Their main advantages lies in anonymity, decentralization and lower costs of electronic transactions. On the other hand, this same "loose" regulation can facilitate black market activities and tax avoidance. One of the drawbacks also attributed to cryptocurrencies is their exceptional volatility. It is, however, trying to be reduced by developing a number of mathematical models that, combined with technical analysis, can help predict cryptocurrency price movements with greater accuracy. The world economy is constantly changing, and cryptocurrencies could become part of electronic savings over time. In general, the cryptocurrency market is actively growing, as well as the number of their investors, new companies and infrastructure projects related to them are emerging, which can be seen globally, but as well as in small open economies such as the Republic of Croatia whose companies are not lagging behind in innovation in the field of cryptotechnology.

Key words: cryptocurrency, mining, cryptocurrency innovation, regulation

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija.

Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog izvora, te da nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

(vlastoručni potpis studenta)

(mjesto i datum)

STATEMENT ON THE ACADEMIC INTEGRITY

I hereby declare and confirm by my signature that the final thesis is the sole result of my own work based on my research and relies on the published literature, as shown in the listed notes and bibliography.

I declare that no part of the thesis has been written in an unauthorized manner, i.e., it is not transcribed from the non-cited work, and that no part of the thesis infringes any of the copyrights.

I also declare that no part of the thesis has been used for any other work in any other higher education, scientific or educational institution.

(personal signature of the student)

(place and date)

SADRŽAJ

1. UVOD	1
1.1. Predmet i cilj rada	1
1.2. Izvori i metode prikupljanja podataka	1
1.3. Struktura rada	2
2. TEMELJNE KARAKTERISTIKE KRIPTOVALUTA I BLOCKCHAIN TEHNOLOGIJE	3
2.1. Stvaranje kriptovaluta u blockchain tehnologiji	3
2.1.1. Rudarenje	3
2.1.2. Rizici i troškovi rudarenja	7
2.2. Kriptografski mehanizmi vezani uz kriptovalute	9
2.2.1. Kriptografske hash funkcije	9
2.2.2. Hash pokazivači	10
2.2.3. Digitalni potpisi	12
2.2.4. Kriptonovčanici i pohrana kriptovaluta	13
2.2.5. Pametni ugovori	14
2.3. Analiza prednosti i nedostataka kriptovaluta	16
2.3.1. Prednosti kriptovaluta	16
2.3.2. Nedostaci kriptovaluta	18
3. PODRUČJA I NAČIN PRIMJENE KRIPTOVALUTA	20
3.1. Temeljne kriptovalute prema tržišnoj kapitalizaciji	20
3.1.1. Kriptovalute, altcoini i digitalni tokeni	23
3.1.2. Burze kriptovaluta	25
3.2. Svakodnevna upotreba kriptovaluta	27
3.3. Primjeri zemalja koje uvode digitalne valute središnjih banaka	29
3.3.1. Digitalne valute čija upotreba nije sasvim zaživjela	30

3.3.2.	Digitalne valute na čijem se uvođenju aktivo radi	32
3.4.	Temeljni pokazatelji vrijednosti kriptovaluta pri kriptotrgovanju	34
3.4.1.	Indeks relativne snage (engl. Relative Strength Index)	35
3.4.2.	Bollingerove ovojnice (engl. Bollinger Bands)	37
3.4.3.	Fibonaccijeve razine povlačenja (engl. Fibonacci Retracement Levels)	39
3.4.4.	Pomični prosjeci (engl. Moving Averages)	41
4.	RAZVOJ TRŽIŠTA KRIPTOVALUTA U HRVATSKOJ	44
4.1.	Razvoj regulatornog okvira kriptovaluta u Hrvatskoj	44
4.2.	Primjeri hrvatskog poslovanja na tržištu kriptovaluta	46
4.3.	Primjeri izdavanja kriptokovanica u Republici Hrvatskoj	49
4.4.	Mogućnost uvođenja digitalne valute središnjih banaka u Hrvatskoj	51
4.4.1.	Uvođenje digitalne kune	52
4.4.2.	Uvođenje digitalnog eura	53
5.	ZAKLJUČAK	56
	LITERATURA	57
	POPIS INTERNETSKIH STRANICA	61
	POPIS SLIKA	63
	POPIS TABLICA	63
	POPIS GRAFIKONA	63
	ŽIVOTOPIS	64

1. UVOD

Kriptovalute novi su oblik digitalne imovine koja se javlja kao oblik ulaganja, ali i kao sredstvo razmjene. Ovo posljednje čini ih sličnima novcu, ali onomu koji nije vezan za centralne ili poslovne banke niti se kao takav može koristiti kao zakonsko i definitivno sredstvo plaćanja. Kriptovalute nastaju na temelju složenih kriptografskih algoritama čije su tehnike bazirane na blockchain tehnologiji. Budući da je upravo blockchain tehnologija sastavni dio danas aktualne četvrte industrijske revolucije, kriptovalute utjecat će na sve aspekte društva, ekonomske, političke, društvene i kulturološke. Svjetska se ekonomija konstantno mijenja, a kriptovalute mogle bi s vremenom postati dio uobičajene elektroničke štednje. Općenito, tržište kriptovaluta aktivno raste, kao i broj njihovih ulagača, pojavljuju se nove tvrtke i infrastrukturni projekti povezani s njima. Kriptovalute potiču gospodarski razvoj u cijelom svijetu pružajući puno lakši pristup kapitalu i financijskim uslugama pridonoseći transparentnosti, smanjenju transakcijskih troškova i vremena te većoj financijskoj uključenosti i mikrofinanciranju.

1.1. Predmet i cilj rada

Prvenstveni cilj rada jest istražiti relevantne karakteristike blockchain tehnologije i kriptovaluta s posebnim naglaskom na one koje imaju najveću tržišnu kapitalizaciju. Nadalje, analizirat će se tehnički proces nastanka kriptovaluta i temeljni pokazatelji vrijednosti kriptovaluta pri kriptotrgovanju te konačno, koji je utjecaj kriptovaluta na pojedina svjetska tržišta. Rad teži tome da omogući bolje razumijevanje karakteristika i načina trgovanja kriptovalutama, bolje razumijevanja pokazatelja koje investitori koriste pri predviđanju kretanja cijena kriptovaluta te da se pruži uvid u rasprostranjenost i inovacije kriptovaluta u svjetskom gospodarstvu. Također će se pokušati objasniti pojmovi koji su povezani s kriptovalutama i blockchain tehnologijom poput rudara i rudarenja, ICO-a, *hash* funkcija, privatnih i javnih ključeva te kriptonovčanika te će se istaknuti potencijalne prednosti i mane kriptovaluta.

1.2. Izvori i metode prikupljanja podataka

Rad se temelji na sekundarnim izvorima podataka koji obuhvaćaju statističke baze podataka. Osim toga, korišteni su svjetski, znanstveni i stručni članci, udžbenici iz područja kriptotehnologije, financijski časopisi, izvješća o istraživanju tržišta, web-stranica industrije,

baze podataka povezane s industrijom te kratki izvještaji financijskih institucija. Od metoda su korištene općepoznate metode poput induktivne metode kako bi se donijeli opći zaključci na temelju pojedinačnih prikupljenih podataka te deduktivna metoda kako bi se donijeli pojedinačni zaključci. Pomoću metode analize složeni pojmovi raščlanjeni su na njihove jednostavnije elemente, a pomoću metode sinteze proučavani dijelovi povezat će se u jednu cjelinu. Povijesna metoda bit će korištena kako bi se utvrdili mogući razlozi kretanja pokazatelja. Metoda komparacije omogućit će usporedbu pokazatelja na promatranim tržištima. Metodom tehničke analize analiziralo se stvaranje kriptovaluta, kriptopokazatelji i podaci tržišnih kretanja.

1.3. Struktura rada

Diplomski rad podijeljen je na pet poglavlja. U *Uvodu* se daje uvid u predmet i cilja rada, izvore i metode prikupljanja podataka te u to kako je diplomski rad koncipiran te kratak sažetak pojedinih poglavlja. U poglavlju *Temeljne karakteristike kriptovaluta i blockchain tehnologije* objašnjena je temeljna terminologija i pojmovi kroz definicije i primjere te su navedene elementarne karakteristike kriptovaluta i blockchain tehnologije. Ovdje su također analizirane prednosti i nedostaci kriptovaluta te je pojednostavljenom terminologijom objašnjen proces rudarenja. Težište diplomskog rada nalazi se u poglavlju *Područja i način primjene kriptovaluta* gdje je analiziran utjecaj kriptovaluta na svjetska tržišta te su ukratko su objašnjeni osnovni kriptopokazatelji, njihova svojstva i grafički su prikazani. Nadalje, u poglavlju *Razvoj tržišta kriptovaluta u Hrvatskoj* navedeni su primjeri hrvatskih kriptoinovacija i pokušaj njihove regulacije. U *Zaključku* će se osvrnuti na najbitnije spoznaje diplomskoga rada. Na kraju rada nalazi se i popis korištene literature te popis ilustracija i tablica korištenih tijekom pisanja u slučaju da čitatelja u vezi s temom zanima više nego što je u diplomskome radu obrađeno.

2. TEMELJNE KARAKTERISTIKE KRIPTOVALUTA I BLOCKCHAIN TEHNOLOGIJE

2.1. Stvaranje kriptovaluta u blockchain tehnologiji

Blockchain je temeljna tehnologija kriptovaluta i njegov cilj bio je, prema njegovim osnivačima¹, ponuditi alternativu bankama kako bi se zaštitili od nove financijske krize. Smatra se da je ključna prednost blockchaina decentralizacija, što može pomoći u uspostavljanju intermedijarnih peer-to-peer (P2P) transakcija, koordinacije i suradnje u distribuiranim sustavima bez centralizirane kontrole među pojedincima, na temelju tehnika poput šifriranja podataka, kriptografije te algoritama distribuiranog konsenzusa. Kao takav blockchain može ponuditi novo rješenje za dugogodišnje probleme visokih operativnih troškova, niske učinkovitosti i potencijalnih sigurnosnih rizika pohrane podataka u tradicionalnim centraliziranim sustavima. Blockchain se može smatrati sljedećom generacijom računalstva u oblaku i očekuje se da će radikalno preoblikovati model ponašanja pojedinaca i organizacija i tako ostvariti prijelaz s današnjeg Interneta informacija na budući Internet vrijednosti. Nadalje, prema Yuanu i Yangu² za blockchain se kaže da je distribuirana zajednička knjiga (engl. *distributed shared ledger*) u kojoj se provjera, pohrana, održavanje i prijenos blockchain podataka temelje na distribuiranoj arhitekturi, a međusobno povjerenje među distribuiranim čvorovima uspostavlja se putem matematičkih algoritama. Ona sadrži niz kronoloških brojeva koji se kronološki povećavaju nakon svake transakcije. Svaki od računa također ima zasebni broj koji sadrži samo binarne znamenke koje se odnose na vlasništvo, ugovore, što daje najveću anonimnost korisnika kriptovaluta. Štoviše, ovi se kodovi ažuriraju nakon svake transakcije, čiji se podaci pohranjuju se na blockchainu u obliku ulančanih blokova s vremenskim oznakama. Razne vrste mehanizama ekonomskih poticaja osmišljene kako bi se proširila zajednica blockchain rudara, tako da su ti rudari spremni sudjelovati u provjeri blokova podataka u distribuiranoj zajedničkoj knjizi. O njihovoj izuzetnoj važnosti bit će više riječi dalje u tekstu.

2.1.1. Rudarenje

Umjesto na određeno centralizirano tijelo izdavanje kriptovaluta oslanja se na konsenzusnu

¹ Iako se Satoshi Nakamoto pretpostavlja kao osnivač bitcoina i blockchain tehnologije, još uvijek se ne zna predstavlja li ovaj pseudonim jednu ili više osoba.

² Yuan, Y. i Wang, F. Y. (2018) Blockchain and cryptocurrencies: Model, techniques, and applications. *IEEE* 48(9), str. 1421.

konkurenciju među distribuiranim mrežnim čvorovima poznato kao rudarstvo temeljeno na provjeri rada (engl. *proof-of-work*³). U ovom procesu temeljenom na PoW-u svaki računalni čvor u P2P mreži doprinosi svojim računalnim resursima i natječe se u rješavanju matematičkog problema. Ono što privlači mnoge rudare (engl. *miners*) jest mogućnost nagrađivanja kriptovalutom odnosno bitcoinom⁴. Bitcoin nagrada koju rudari dobivaju poticaj je koji motivira ljude da pomognu u primarnoj svrsi rudarstva: ozakonjenju i praćenju bitcoin transakcija osiguravajući njihovu valjanost. Budući da su ove odgovornosti raspodijeljene među mnogim korisnicima diljem svijeta, bitcoin je "decentralizirana" kriptovaluta koja se ne oslanja ni na kakvu središnju vlast poput središnje banke koja bi nadgledala njezinu regulaciju. Provjerom transakcija rudari pomažu u sprječavanju "problema dvostruke potrošnje", gdje vlasnik bitcoina nezakonito troši isti bitcoin dva puta. S fizičkom valutom to nije problem: kad jednom nekome predamo novčanicu od 20 dolara, više ju nemamo, pa nema opasnosti da se tom istom novčanicom od 20 dolara kupi štogod drugo. Međutim, s digitalnom valutom postoji rizik da bi imatelj mogao napraviti kopiju digitalnog tokena i poslati ga trgovcu ili drugoj strani zadržavajući original. Nakon što rudari provjere bitcoin transakcije u vrijednosti od 1 MB⁵ (megabajta) odnosno "blok", ti rudari mogu biti nagrađeni s određenom količinom bitcoina. Ipak, da bi zaradio bitcoin, rudar mora ispuniti dva uvjeta: 1) mora potvrditi transakcije u vrijednosti od 1 MB i 2) mora biti prvi rudar koji je došao do pravog odgovora ili najbližeg odgovora na matematički problem (već spomenuti PoW).

Slika 1. Uvjeti bitcoin rudarenja



Izvor: Sabrina Jiang © Investopedia (2020). Dostupno na: <https://www.investopedia.com/tech/how-does-bitcoin-mining-work/>

³ Dalje će se u radu koristiti kratica PoW.

⁴ Proces rudarenja objasniti ćemo rudarenjem bitcoina.

⁵ Ograničenje od 1 MB postavio je Satoshi Nakamoto. Međutim, neki rudari vjeruju da bi trebalo povećati veličinu bloka kako bi se primilo više podataka, što bi značilo da bi bitcoin mreža mogla brže obrađivati i provjeravati transakcije.

Rješavanje ovog problema sastoji se u pogađanju 64-znamenkastog heksadecimalnog broja (engl. *hash*⁶) koji je manji ili jednak ciljanomu (engl. *target hash*). Na ovaj način rudari služe svojoj vitalnoj svrsi – puštanju kriptovaluta u optjecaj. Drugim riječima, rudari u osnovi "kuju" valutu. Svaki bitcoin nastao je zbog rudara, osim kovanica prvog bloka (engl. *genesis block*) koji je stvorio osnivač Satoshi Nakamoto. Kada rudara više ne bi bilo, bitcoin mreža i dalje bi postojala i bila upotrebljiva, ali ne bi više bilo dodatnih bitcoina. Valja istaknuti da je ukupan broj bitcoina ograničen na 21 milijun⁷, a stopa rudarenih bitcoina s vremenom se smanjuje.⁸ Međutim, to ne znači da će transakcije prestati biti verificirane. Rudari će i dalje provjeravati transakcije i za to će im biti plaćene naknade kako bi zadržali integritet bitcoin mreže. Nagrade za rudarenje bitcoina smanjuju se za polovicu svake četiri godine, odnosno nakon svakog 210.000. bloka. Prvim rudarenjima u 2009. godini moglo se zaraditi 50 BTC, u 2012. godini to je prepolovljeno na 25 BTC te u 2016. na 12,5 BTC. Danas nagrada iznosi 6,25 BTC⁹.

Grafikon 1. Smanjenje nagrade za rudarenje nakon svakog 210.000. bloka



Izvor: Sabrina Jiang © Investopedia (2020). Dostupno na: <https://www.investopedia.com/tech/how-does-bitcoin-mining-work/>

⁶ *Hash* je funkcija koja pretvara input slova i brojeva u šifrirani output fiksne duljine. Stvara se pomoću algoritma i neophodan je za upravljanje blockchainom u kriptovaluti.

⁷ Bitcoin. FAQ. Dostupno na: <https://bitcoin.org/en/faq#how-are-bitcoins-created>

⁸ Pretpostavlja se da će zadnji bitcoin ući u optjecaj tek oko 2140. godine.

⁹ Zadnja redukcija vrijednosti bila je 11. svibnja 2020.

Slika 2. Kriteriji valjanosti bloka

How to win for a given block			
Target	Disqualified	Disqualified	Viable
00000000 00000000 <u>057FCC70</u> 8CF0130D 95E27C58 19203E9F 967AC56E 4DF598EE	00000000 00000000 <u>3</u> 57FCC70 8CF0130D 95E27C58 19203E9F 967AC56E 4DF598EE	00000000 00000000 0 <u>D</u> 7FCC70 8CF0130D 95E27C58 19203E9F 967AC56E 4DF598EE	00000000 00000000 0 <u>4</u> 7FCC70 8CF0130D 95E27C58 19203E9F 967AC56E 4DF598EE
	Has only 16 zeros. (the target has 17). So all right answers need to have at least 17 zeros.	18 th digit it's a "d," which in hexadecimal is 13. This is larger than the 18 th digit of the target — "5."	Smaller than the target hash. Get there before any other miner and get paid 12.5 BTC.

Izvor: Sabrina Jiang © Investopedia (2020). Dostupno na: <https://www.investopedia.com/tech/how-does-bitcoin-mining-work/>

Korištenje outputa fiksne duljine povećava sigurnost jer svatko tko pokušava dešifrirati *hash* neće moći reći koliko je dugačak ili kratak ulaz samo gledajući duljinu izlaza. Rješavanje *hasha* započinje podacima dostupnim u zaglavlju bloka i u osnovi rješava složeni matematički problem. Svako zaglavlje bloka sadrži broj verzije, vremensku oznaku, *hash* upotrijebljen u prethodnom bloku, *nonce* i *target hash*. Ako je novi *hash* manji ili jednak ciljnom *hashu*, tada se prihvaća kao rješenje, rudaru se dodjeljuje nagrada, a blok se dodaje u blockchain.

U bitcoin-mreži često se javljaju situacije kada postoji više točnih odgovora, ali na kraju dana može biti samo jedan „pobjednički“ odgovor. Kada se predstavi više točnih odgovora koji su jednaki ili manji od ciljanog broja, bitcoin-mreža običnom će većinom (51%) odlučiti kojeg će rudara nagraditi. Obično je rudar ili rudarski bazen koji je odradio najviše posla ili, drugim riječima, onaj koji verificira najviše transakcija te tako doprinosi bitcoin-zajednici. Gubitnički blok tada postaje "blok siročić" (engl. *orphan block*¹²). Rudari koji uspješno riješe problem *hasha*, ali koji nisu provjerili većinu transakcija, ne nagrađuju se bitcoinima.

2.1.2. Rizici i troškovi rudarenja

Rizici: Rizici rudarstva su financijski i regulatorni.

- 1) Regulatorni - Zakonitost rudarenja kriptovaluta ovisi o zemljopisnom položaju. Koncept kriptovaluta može ugroziti dominaciju fiat valuta i vladinu kontrolu nad financijskim tržištima. Iz tog su razloga na nekim mjestima potpuno ilegalane iako je njihova upotreba i

¹² *Orphan blocks* ili blokovi siročić blokovi su koji se, iako imaju točno rješenje, ne dodaju u lanac.

rudarenje legalno u većini svijeta. Prema *Law Library of Congress (2018)*¹³ kriptovalute su ilegalne u Alžiru, Egipatu, Maroku, Boliviji, Ekvadoru, Nepal i Pakistanu. Stoga se preporuča istražiti propise matičnih zemalja prije ulaganja u rudarsku opremu i/ili kriptovalute.

- 2) Financijski – Financijski rizik sastoji se u činjenici da osoba može proći sav napor da kupi rudarsku opremu vrijednu stotine ili tisuće dolara a da pritom ne ostvari povrat na svoje ulaganje. Ipak, ovaj se rizik može ublažiti pridruživanjem rudarskih bazena (engl. *mining pools*). S obzirom na to da je vjerojatnost da će pojedinac biti taj koji će otkriti rješenje jednaka udjelu ukupne rudarske snage na mreži, sudionici s malim postotkom rudarske snage imaju vrlo male šanse da sami otkriju sljedeći blok. Uzevši to u obzir, moglo bi proći puno vremena prije nego što rudar pronade blok, a poteškoće se s vremenom povećavaju. Iz tog razloga rudar pojedinac možda nikada neće nadoknaditi uloženo. Odgovor na ovaj problem su rudarski bazeni. Rudarskim bazenima upravljaju treće strane i koordiniraju grupe rudara radeći zajedno u „bazenu“ i dijeleći isplate među svim sudionicima.

Troškovi: U povijesti kriptovaluta pojedinci su se mogli natjecati za blokove pomoću uobičajenog kućnog računala, ali danas to više nije slučaj jer se poteškoća rudarenja mijenja s vremenom. Kako bi se osiguralo nesmetano funkcioniranje blockchaina i njegova sposobnost obrade i provjere transakcija, teži se proizvesti jedan blok svakih 10-ak minuta. Međutim, ako se milijun rudarskih platformi natječe u rješavanju problema, vjerojatno će doći do rješenja brže od scenarija u kojem 10 rudarskih postrojenja radi na istom problemu. Iz tog razloga, bitcoin je dizajniran za procjenu i prilagodbu poteškoća rudarenja svakih 2.016 blokova ili otprilike svaka dva tjedna. Kada postoji više računarske snage koja zajednički radi na iskopavanju bitcoina, razina poteškoća rudarstva povećava se kako bi se blok proizvodnja održala na stabilnoj brzini. To znači da rudari, kako bi mogli biti konkurentni, moraju ulagati u moćnu računalnu opremu poput GPU-a (engl. *graphics processing unit*) ili ASIC-a (engl. *application-specific integrated circuit*) čija se cijena može kretati od 500 do desetke tisuća dolara. Nadalje, ne samo da rudari moraju uzimati u obzir troškove povezane sa skupom opremom potrebnom da bi imali šanse za rješavanje *hash* problema već moraju uzeti u obzir značajnu količinu opreme za eksploataciju električne energije koja se koristi u stvaranju ogromnih količina novčanih sredstava u potrazi za rješenjem. Konačno, rudarstvo bitcoina većinom nije isplativo za većinu pojedinačnih rudara.

¹³ The Law Library of Congress (2018) *Regulation of Cryptocurrency Around the World*. Washington: Global Legal Research Center, str. 7-124.

2.2. Kriptografski mehanizmi vezani uz kriptovalute

Svaka valuta treba neku vrstu kontrole ponude i provođenje različitih sigurnosnih mjera kako bi se spriječile prevare. Kod fiat valuta institucije poput središnjih banaka kontroliraju novčanu masu i borbe se protiv krivotvorenja, ali to i dalje ne čini novac nemogućim za krivotvorenje. Kriptovalute također moraju imati sigurnosne mjere koje sprječavaju ljude da se miješaju u sustav i daju međusobno nedosljedne izjave različitim ljudima. Kao što riječ sugerira, kriptovalute temelje se na kriptografiji¹⁴ koja pruža mehanizam za sigurno kodiranje pravila sustava kriptovaluta u samom sustavu, a čije ćemo glavne mehanizme objasniti dalje u tekstu.

2.2.1. Kriptografske hash funkcije

Hash funkcija matematička je funkcija koja pretvara numeričku ulaznu vrijednost ili *input* u drugu komprimiranu numeričku vrijednost te ima sljedeća svojstva¹⁵:

- *Input* funkcije može biti bilo koji niz bilo koje veličine, ali generira *output* fiksne veličine, konkretno 256-bitnu veličina *outputa*.
- U funkciji ne postoji kolizija.
- Funkcija sadrži svojstvo „skrivanja“ (engl. *hiding property*)

Svojstvo 1. Otpornost na kolizije. Do kolizije dolazi kada dva različita *inputa* daju isti *output*. Kaže se da je *hash* funkcija *H* otporna na koliziju ako nitko ne može pronaći koliziju, odnosno ako vrijedi da je nemoguće pronaći vrijednosti *x* i *y*, tako da $x \neq y$ i $H(x) = H(y)$.

Valja istaknuti kako kolizije u kriptografiji zapravo postoje i njih je moguće dokazati posebnim algoritmima jer budući da *input* sadrži sve nizove svih duljina, a *output* sadrži samo nizove određene fiksne duljine, tada mora postojati niz *inputa* koji su jednaki istom *outputu*. Međutim, kako računalo računa 10.000 *hash/sec*, tako bi trebalo više od jedne kvadrtrilijarde (10^{27}) godina da se izračuna 2^{128} *hashova*! Zbog ove astronomske brojke uzima se da su šanse da bi pronašli koliziju beskrajno malene.

¹⁴ Kriptografija je istraživačko područje dubokog učenja koje koristi mnoge napredne matematičke tehnike koje pružaju temeljne usluge informacijske sigurnosti.

¹⁵ Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016) *Bitcoin and Cryptocurrency Technologies*. Princeton: Princeton University, str. 23-30.

Svojstvo 2. Skrivanje. *Hash* funkcija je skrivena ako: kada se odabere tajna vrijednost r iz distribucije vjerojatnosti koja ima visoku minimalnu entropiju¹⁶, tada je s obzirom na $H(r \parallel x)$ nemoguće pronaći x , što konkretno znači da ne postoji određena vrijednost koja ima veću vjerojatnost za pojavljivanje.

Ovo se svojstvo koristi pri shemi koju nazivamo shema predanosti ili engl. *commitment scheme*. Da bi se koristila shema predanosti, prvo treba generirati slučajni *nonce*¹⁷. Zatim se na ovu vrijednost primjenjuje funkciju zajedno s *msg* ili porukom. Konačno, svatko može provjeriti je li poruka doista ranije i predana.

Commitment scheme. Sastoji se od dva algoritma:

- **com:=commit (msg, nonce)** Algoritam uzima poruku i tajno slučajnu vrijednost, koja se naziva *nonce*, kao *input* i vraća *commitment*.
- **verify(com, msg, nonce)** Algoritam vraća *true* ako je $com == commit(msg, nonce)$ i *false* u suprotnom.

Funkcija koja se koristi za generiranje *hasha* je deterministička, što znači da će proizvesti isti rezultat svaki put kada se koristi isti ulaz. To također znači da funkcija može učinkovito generirati output te otežava određivanje inputa (što dovodi do rudarenja) tako što unosi malih promjena rezultiraju vrlo različitim *hashom*.

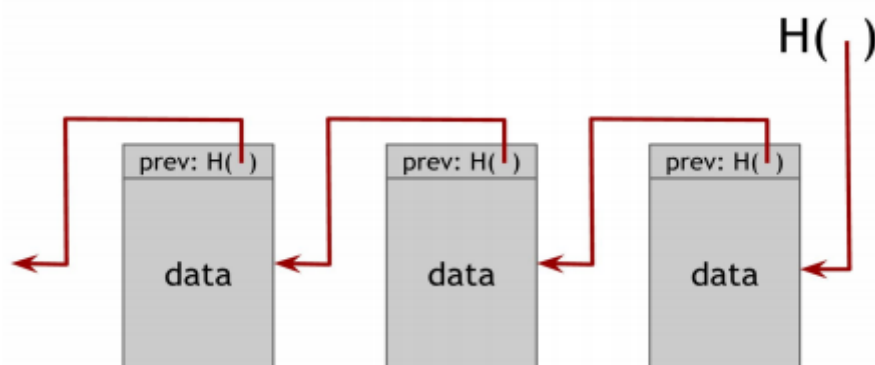
2.2.2. Hash pokazivači

Pokazivač hash jest pokazivač na mjesto gdje se neke informacije pohranjuju zajedno s kriptografskim *hashom* podataka. Dok obični pokazivač samo daje pristup za dohvaćanje informacija, *hash* pokazivač također omogućuje potvrđivanje da se podaci nisu promijenili. Na Slici 3. prikazan je blockchain čiji su blokovi povezani *hash* pokazivačima. Tako svaki blok ne samo da govori gdje se nalazi vrijednost prethodnog bloka već sadrži i sažetak te vrijednosti koji omogućuje da se potvrdi kako se vrijednost nije promijenila.

¹⁶ Minimalna entropija mjeri koliko je ishod predvidiv, a visoka minimalna entropija bilježi intuitivnu ideju da je distribucija (tj. slučajna varijabla) vrlo raširena.

¹⁷ U kriptografiji se izraz *nonce* koristi za označavanje vrijednosti koja se može koristiti samo jednom.

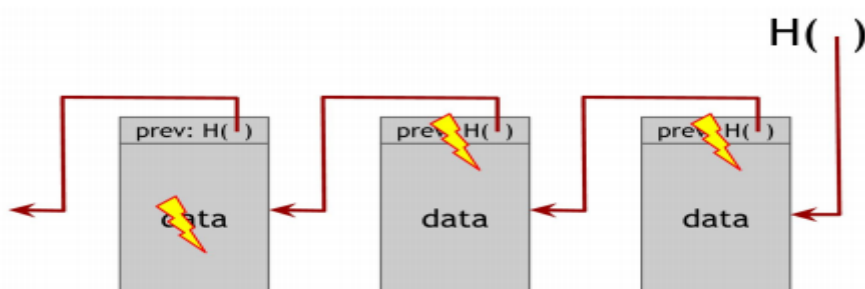
Slika 3. *Hash* pokazivači u blockchainu



Izvor: Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016) *Bitcoin and Cryptocurrency Technologies*. Princeton: Princeton University, str. 33

Hash pokazivači koriste se za otkrivanje neovlaštenih mijenjanja informacija, odnosno pomoću njih se gradi struktura podataka koja pohranjuje golem broj podataka i omogućuje nam neprestano dodavanje novih na kraj. Ako netko promijeni podatke koji su ranije zabilježeni, to se može otkriti. Modificiranje podataka bilo gdje u lancu blokova, rezultirat će netočnim pokazivačem u sljedećem bloku. Čak i ako protivnik izmijeni sve pokazivače kako bi bili u skladu s izmijenjenim podacima, pokazivač u zaglavlju bit će netočan te se može uspješno otkriti neovlašteno modificiranje.

Slika 4. Otkrivanje neovlaštenih mijenjanja informacija *hash* pokazivačima



Izvor: Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016) *Bitcoin and Cryptocurrency Technologies*. Princeton: Princeton University, str. 34

Hash pokazivači također se koriste s digitalnim potpisima. Potpisivanjem *hash* pokazivača potpis pokriva ili štiti cijelu strukturu - ne samo sam *hash* pokazivač već i sve na što ukazuje lanac *hash* pokazivača. Na primjer, potpisivanje *hash* pokazivača koji se nalazio na kraju lanca blokova rezultirat će digitalnim potpisivanjem cijelog lanca blokova.

2.2.3. Digitalni potpisi

Digitalni potpis zamišljen je kao potpis na papiru, ali u digitalnom obliku. Ono što se ovom vrstom potpisa želi postići jest da se samo pojedinac kojemu potpis pripada može potpisati na određeni dokument ili potpisom potvrditi transakciju, ali svatko tko vidi taj potpis može provjeriti je li valjan. Također se želi postići da bilo tko ne može kopirati taj potpis s jednog dokumenta na drugi s obzirom na to da potpis označava pristanak ili odobrenje određenog dokumenta. Kako bismo to postigli, koristimo se shemom digitalnog potpisa koja se sastoji od sljedeća tri algoritma¹⁸:

- $(sk, pk) := generateKeys$ (veličina ključa) **Metoda generiranja ključeva** uzima veličinu ključa i generira par ključeva. Tajni ključ sk (engl. *secret key*) čuva se privatno i koristi se za potpisivanje poruka. pk (engl. *public key*) javni je ključ za provjeru koji se daje svima. Svatko s ovim ključem može provjeriti ovaj potpis.
- $sig := sign(sk, message)$ **Metoda potpisivanja** uzima poruku i tajni ključ kao *input* i generira potpis za poruku pod tajnim ključem.
- $isValid := verify(pk, message, sig)$ **Metoda provjere** uzima kao *input* poruku, potpis i javni ključ. Vraća logičku vrijednost, $isValid$, koja će biti istinita ako je sig važeći potpis za poruku pod javnim ključem pk , a u suprotnom neistinita.¹⁹

U ovakvom sustavu javni ključevi djeluju kao identiteti. Posljedica postupanja s javnim ključevima kao identitetima jest ta da pojedinac može izraditi novi identitet kad god poželi - stvaranjem novog para ključeva, sk i pk , pomoću *generateKeys* algoritma. pk je novi javni identitet, a sk je odgovarajući tajni ključ.

Prema Dujelli²⁰ „korištenje originalne poruke u generiranju digitalnog potpisa često rezultira vrlo dugačkim potpisom. Stoga se umjesto originalne poruke često koristi "sažetak poruke" (engl. *message digest*) koji se dobije primjenom neke *hash* funkcije.“ Postoje kriptosustavi s javnim ključem koji se mogu direktno koristiti za potpisivanje poruke. Međutim, najpoznatije metode za generiranje digitalnih potpisa jesu Digital Signature Algorithm (DSA/DSS) koja je zasnovana na problemu diskretnog logaritma u multiplikativnoj grupi konačnog polja i Elliptic

¹⁸ Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016) *Bitcoin and Cryptocurrency Technologies*. Princeton: Princeton University, str. 37

¹⁹ Napomena: *generateKeys* i *sign* slučajni su algoritmi, čime se povećava sigurnost transakcija. *verify* će, s druge strane, uvijek biti deterministički.

²⁰ Dujella, A. (2003) *Elliptic Curve Digital Signature Algorithm*. Predavanje iz kolegija Eliptičke krivulje i njihova primjena u kriptografiji. Zagreb: Prirodoslovno-matematički fakultet

Curve Digital Signature Algorithm (ECDSA) koji predstavlja njegov analogon i koristi eliptičke krivulje.

2.2.4. Kriptonovčanici i pohrana kriptovaluta

Kako bi trgovao kriptovalutom, pojedinac mora znati neke javne podatke i neke tajne podatke. Javne informacije su ono što se nalazi na blockchainu - identitet kovanice, koliko vrijedi itd. Tajni podaci tajni su ključ vlasnika bitcoina. Pohranjivanje kriptovalute sastoji se od pohrane i upravljanja tajnim ključevima. Najjednostavnija metoda upravljanja ključevima je pohranjivanje na lokalni uređaj: računalo ili pametni telefon. Iako je ova metoda iznimno praktična jer omogućuje trošenje kovanica pritiskom samo nekoliko gumba, sigurnost opada. Naime, ako se uređaj izgubi ili ako se datoteka ošteti, ključevi će se izgubiti, a i kovanice. Također, ako netko ukrade ili provali u uređaj ili ga zarazi *malwareom*, može kopirati ključeve, a zatim sve kovanice poslati sebi. Ako se kriptovaluta pohranjuje lokalno, obično se koristi softver novčanika koji prati sve novčiće i upravlja svim detaljima ključeva.

Za trgovanje kriptovalutom potreban je način razmjene adresa s drugom stranom - adresa na koju se trebaju poslati kovanice. Postoje dva glavna načina na koje se adrese šalju: kao tekstualni niz ili kao QR kôd. Da bi se adresa kodirala kao tekstualni niz, uzimamo bitove ključa i pretvaramo ga iz binarnog broja u osnovni 58-znamenasti broj. Zatim se koristi skup od 58 znakova za kodiranje svake znamenke kao znaka, što se naziva notacija *base58*²¹, što omogućuje čitanje kodiranih adresa putem telefona. Druga metoda za kodiranje adrese jest QR kôd, jednostavna vrsta dvodimenzionalnog crtičnog koda. Prednost QR koda jest što ga se može slikati pametnim telefonom, a softver novčanika može automatski pretvoriti crtični kôd u niz bitova koji predstavlja odgovarajuću adresu.²²

Nadalje, kriptonovčanike moguće je podijeliti na vruće (engl. *hot wallets*) i hladne (engl. *cold wallets*). Vruće kriptonovčanike dalje je moguće podijeliti na novčanike na radnoj površini računala (npr. Exodus), mobilne novčanike (npr. Edge ili Trust Wallet) te hibridne novčanike (npr. BTCPay). Pod hladne novčanike podrazumijevamo papirnate novčanike (engl. *paper wallets*) te hardware novčanike poput Trezora ili SafePala. Ključna razlika između vrućeg i hladnog novčanika je u tome što su vrući novčanici povezani s internetom, dok hladni novčanici

²¹ Broj 58 se koristi jer je to broj koji dobivamo kada uključujemo velika i mala slova, kao i znamenke i znakove, ali izostavljamo neke koji bi mogli zbuniti ili izgledati poput drugog znaka. Naprimjer, veliko slovo 'O' i nula izostavljeni su jer izgledaju previše slično.

²² To je korisno u trgovini: sustav odjave može prikazati QR kôd i telefonom možete platiti skeniranjem koda i slanjem kovanica na tu adresu. Također je korisno za prijenos valuta na telefon.

nisu. Kao rezultat toga, hladni novčanici smatraju se sigurnijom opcijom pohrane digitalne imovine. Vrući novčanici namijenjeni su svakodnevnim korisnicima kriptovaluta, primjerice onima koji redovito trguju kriptovalutama na burzi ili ih troše za svakodnevne kupnje. Pohranjivanje velike količine digitalne imovine u vrući novčanik, kao što je web novčanik ili mobilni novčanik, nije preporučljivo jer je imovina tada izložena potencijalnim sigurnosnim prijetnjama poput cyber krađe. Hladni novčanici smatraju se sigurnijim rješenjem za pohranu kriptovaluta jer nisu povezani s internetom. Hardverski novčanici koriste fizički medij - obično u obliku USB sticka - za pohranu privatnih ključeva novčanika, čineći ih de facto nedostupnima hakerima ili drugim zlonamjernim stranama. Papirnatih novčanici funkcioniraju na sličan način kao i hardverski novčanici. Međutim, umjesto fizičkog uređaja sličnog USB-u papirnatih novčanici su papiri koji sadrže javnu adresu novčanika i privatni ključ. Za slanje kovanica iz papirnato novčanika novčanik se mora uvesti u vrući novčanik skeniranjem privatnih ključeva kako bi se novac u njemu mogao potrošiti. Iako hladni novčanici pružaju vrhunsko rješenje za pohranu u sigurnosnom smislu, glavni nedostatak je taj što su oni nepraktični za svakodnevnu upotrebu.

Slika 5. Notacija i QR kôd

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa



Izvor: Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016) *Bitcoin and Cryptocurrency Technologies*. Princeton: Princeton University, str. 102

2.2.5. Pametni ugovori

Pametne ugovore prvi je put predložio 1994. godine Nick Szabo, američki informatičar koji je 1998. izumio virtualnu valutu zvanu "Bit Gold". On je definirao pametne ugovore kao kompjuterizirane protokole transakcija koji izvršavaju uvjete ugovora te koji dopuštaju

provođenje pouzdanih transakcija i sporazuma između različitih, anonimnih strana bez potrebe za središnjim tijelom, pravnim sustavom ili vanjskim mehanizmom izvršenja. Pametni ugovori predstavljani su kôdom koji omogućuje razmjenu nakon što se ispune unaprijed utvrđeni uvjeti. Pametni ugovori veliki su pokretač onoga što je poznato kao Internet stvari. Međutim, pametni ugovori također mogu pokrenuti razmjenu na temelju podataka (npr. internetska povezanost računalnih uređaja ugrađenih u svakodnevne predmete, što im omogućuje slanje i primanje podataka.) unesenih u blockchain za automatizirane zadatke. Kod ethereuma pametni ugovor jest program koji nastaje na blockchainu. Svatko može stvoriti ethereum ugovor, za malu naknadu, učitavanjem njegovog programskog koda u posebnu transakciju. Nakon učitavanja ugovor ima vlastiti saldo sredstava te može slati i primati novac.

Na Slici 6. prikazan je jednostavan ethereum ugovor. Kodiran u *Solidityju*, ethereumovom programskom jeziku na visokoj razini za definiranje ugovora, ovim se ugovorom provodi pohranjivanje imena/vrijednosti u registar imena, u kojem se imenima dodjeljuju vrijednosti jednom zauvijek. Ugovorom je definirana podatkovna varijabla, *registryTable*, koja prikazuje preslikavanje 32-bajtnih nizova u javne ključeve. U početku mapira svaki niz na *null* adresu 0x0000000000 ... 000. Ovaj ugovor također definira jedinstvenu ulaznu točku koja se naziva *claimName*. Ova ulazna točka prihvaća jedan argument, ime. Prvo, ugovor osigurava da je pozivatelj poslao vrijednost od najmanje 10 *wei*²³. Ako je poslano nedovoljno sredstava, ugovor se raskida s pogreškom (izjava "*throw*") i ne poduzima se ništa. Ako se pošalje dovoljno sredstava, a ime još nije uzeto, tada će mu se trajno dodijeliti vrijednost bilo koje adrese koja je pozvala ovu funkciju.

Slika 6. Ethereum transakcija

```
contract NameRegistry {
    mapping(bytes32 => address) public registryTable;
    function claimName(bytes32 name) {
        if (msg.value < 10) {
            throw;
        }
        if (registryTable[name] == 0) {
            registryTable[name] = msg.sender;
        }
    }
}
```

Izvor: Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016) *Bitcoin and Cryptocurrency Technologies*. Princeton: Princeton University, str. 287

²³ *Wei* je najmanja novčana jedinica u ethereumu.

2.3. Analiza prednosti i nedostataka kriptovaluta

2.3.1. Prednosti kriptovaluta

Kriptovalute potpuno su decentralizirane bez središnje kontrole ili hijerarhijske strukture. Zapravo, one se kontroliraju distribuiranim konsenzus algoritmima pokrenutim među računalnim čvorovima u P2P mrežama. Tradicionalni elektronički novac, međutim, obično treba centralizirane pružatelje usluga, pa ih stoga centralno kontroliraju vlade ili određene tvrtke. Kriptovalute predstavljaju pouzdano sredstvo razmjene izvan izravne kontrole nacionalnih banaka, poput američkog FED-a ili ECB-a. To je posebno privlačno za ljude koji se brinu da će „kvantitativno labavljenje“²⁴ i drugi oblici labave monetarne politike, poput međubankarskih kamatnih stopa gotovo jednakih nuli, dovesti do dugoročnih ekonomskih nestabilnosti.

Dugoročno gledano, mnogi ekonomisti očekuju da će svjetske vlade prihvatiti kriptovalute ili barem uključiti aspekte kriptovaluta (poput ugrađenih protokola nestašice i provjere autentičnosti) u fiat valute. To bi potencijalno moglo zadovoljiti zabrinutost nekih zagovornika kriptovaluta zbog inflatorne prirode fiat valuta i nesigurnosti fizičkog novca. Primjerice, bitcoin ima ograničeno izdavanje valuta s ograničenjem od oko 21 milijun bitcoina. Dok većina tradicionalnog novca praktički ima neograničeno izdavanje valuta. Centralizirani pružatelj usluga može donijeti odluku o povećanju ili smanjenju ponude gotovine, što bi moglo uzrokovati inflaciju ili deflaciju. Nadalje, privatnost i anonimnost bile su glavni argumenti zagovornika ranih kriptovaluta, a to ostaju i danas. Mnogi korisnici kriptovaluta koriste pseudonime koji nisu povezani s bilo kojim informacijama, računima ili pohranjenim podacima koji bi ih mogli identificirati. Iako je sofisticiranim članovima zajednice moguće utvrditi identitet korisnika, novije kriptovalute imaju dodatne zaštite koje to znatno otežavaju. Suprotno tome, većina tradicionalnog elektroničkog novca nije anonimna, a identitet korisnika evidentirat će centralizirani pružatelji usluga. Međutim, unatoč anonimnosti svatko može provjeriti izvorni kôd kriptovalute, pa će stoga svatko moći i razumjeti osnovne mehanizme njihova izdavanja.

S druge strane, većina tradicionalnih elektroničkih novčanih sredstava zatvorenog je izvora, a kritična poslovna logika uvijek se čuva kao tajna za korisnike. Osim toga, kada građani u represivnim zemljama uđu u konflikt s vladom, te iste vlade mogu lako zamrznuti ili zaplijeniti

²⁴ „Tiskanje novca“ središnjih banaka kupnjom državnih obveznica.

njihove domaće bankovne račune ili stornirati transakcije izvršene u lokalnoj valuti. To je posebno zabrinjavajuće u autokratskim zemljama poput Kine i Rusije, gdje se imućne osobe, koje se suprotstave vladajućim strankama, često suočavaju s ozbiljnim finansijskim i pravnim problemima sumnjiva podrijetla.

Za razliku od fiat valuta koje podržavaju središnje banke kriptovalute praktički su „imune“ na autoritarne hirove. Sredstva i evidencije o transakcijama pohranjuju se na brojnim mjestima širom svijeta, što čini kontrolu države - čak i pod pretpostavkom međunarodne suradnje - krajnje nepraktičnom. Pojednostavljeno se može reći da korištenje kriptovaluta teoretski može djelovati poput posjedovanja neograničenog broja računa u inozemstvu. Decentralizacija je problematična za vlade koje su naviknute koristiti finansijsku polugu kako bi držale elite pod kontrolom. Prema Martucciju (2017)²⁵ „Krajem 2017. godine CoinTelegraph izvijestio je o multinacionalnoj inicijativi za kriptovalute na čelu s ruskom vladom. Ako uspije, inicijativa bi imala dva korisna ishoda za uključene: slabljenje dominacije američkog dolara kao de facto svjetskog sredstva razmjene i omogućavanje vladama sudionicama čvršće kontrole nad sve vrijednijim zalihama kriptovaluta.“ Također, koncepti blockchaine, privatnih ključeva i novčanika učinkovito rješavaju problem dvostruke potrošnje, osiguravajući da tehnološki pametni prevaranti sposobni za dupliciranje digitalnih sredstava ne zloupotrebe nove kriptovalute. Sigurnosne značajke kriptovaluta također uklanjaju potrebu za nezavisnim procesorom plaćanja - poput Visa ili PayPala - za autentifikaciju i provjeru svake elektroničke finansijske transakcije. Zauzvrat, ovo eliminira potrebu za obveznim naknadama za transakcije koje podržavaju rad ovih platnih procesora s obzirom na to da rudari zarađuju nove jedinice valute za svoj rad uz neobavezne naknade za transakcije.

Naknade za transakcije kriptovaluta obično su manje od 1% od vrijednosti transakcije, naspram 1,5% do 3% za procesore plaćanja kreditnim karticama i PayPal. Rudarstvo je ugrađeni mehanizam kontrole kvalitete i nadzora za kriptovalute. Budući da su plaćeni za svoj trud, rudari imaju finansijski udio u vođenju točnih, ažurnih evidencija transakcija, čime osiguravaju integritet sustava i vrijednost valute. Zatim, kriptovalute međunarodne transakcije tretiraju jednako kao i domaće transakcije. Transakcije su besplatne ili dolaze s nominalnom naknadom za transakciju, bez obzira gdje se nalaze pošiljalatelj i primatelj. To je ogromna prednost u odnosu na međunarodne transakcije koje uključuju fiat valute koje gotovo uvijek imaju neke posebne naknade koje se ne primjenjuju na domaće transakcije - poput međunarodnih naknada za kreditne kartice ili bankomata, a izravni međunarodni transferi novca mogu biti vrlo skupi, s

²⁵ Martucci, B. (2017) *What Is Cryptocurrency – How It Works, History & Bitcoin Alternatives* [online]. Henderson: Money Crashers.

naknadama koje ponekad prelaze 10% ili 15% prenesenog iznosa. Konačno, kriptovalute dobivaju na vrijednosti povećanjem korisnika i njihovom predanošću. Što više korisnika vjeruje i koristi kriptovalute, one će imati veću vrijednost, kao što je to u povijesti bilo s novčanicama i uvođenjem fiat novca. Suprotno tome, gotovo sva tradicionalna elektronička novčana sredstva podržana su fiat novcem.

2.3.2. Nedostaci kriptovaluta

Vjerojatno najveći nedostatak i regulatorna zabrinutost oko kriptovaluta jest njihova sposobnost da olakša nezakonite aktivnosti. Mnogo internetskih transakcija na sivom i crnom tržištu denominirano je u bitcoinima i drugim kriptovalutama. Na primjer, zloglasno mračno tržište Silk Road koristilo je bitcoin za olakšavanje ilegalnih kupnji droga i drugih ilegalnih aktivnosti prije nego što je ugašeno 2014. Kriptovalute su također sve popularniji alati za pranje novca - usmjeravanje nezakonito stečenog novca putem posrednika radi prikrivanja njegova izvora. Iste snage koje vladama otežavaju zauzimanje i praćenje kriptovaluta omogućuju kriminalcima da rade s relativnom lakoćom. S druge strane, postoji potencijal za utaju poreza. Budući da kriptovalute ne reguliraju nacionalne vlade i obično postoje izvan njihove izravne kontrole, one prirodno privlače neplatiše poreza. Postoje mali poslodavci koji plaćaju zaposlenike u bitcoinima i drugim kriptovalutama kako bi izbjegli odgovornost za porez na plaću i pomogli svojim radnicima da izbjegnu obvezu poreza na dohodak, dok internetski prodavači često prihvaćaju kriptovalute kako bi izbjegli obveze poreza na promet i dobit. Tako već spomenuta anonimnost kriptovaluta otežava i praćenje poreznih zakona. Štoviše, rani zagovornici kriptovaluta vjerovali su da će, ako budu pravilno osigurane, digitalne alternativne valute biti značajan odmak od fizičke gotovine, koju su smatrali nesavršenom i u osnovi rizičnom.

Uz pretpostavku gotovo neiscrpljivog izvornog koda, neprobojnih protokola provjere autentičnosti (ključeva) i odgovarajuće obrane od hakiranja, sigurnije je novac pohraniti u oblak ili čak u fizički uređaj za pohranu podataka nego u stražnjem džepu ili torbici. Međutim, ovo pretpostavlja da korisnici kriptovaluta poduzimaju odgovarajuće mjere predostrožnosti kako bi izbjegli gubitak podataka. Na primjer, korisnici koji pohranjuju svoje privatne ključeve na pojedinačne fizičke uređaje za pohranu trpe nepovratnu financijsku štetu kad se uređaj izgubi ili ukrade. Čak i korisnici koji svoje podatke pohranjuju s jednom uslugom u oblaku mogu se suočiti s gubitkom ako je poslužitelj fizički oštećen ili odspojen s globalnim Internetom. Osim toga, postoji potencijal za visoku volatilnost i manipulaciju cijenama. Naime, mnoge kriptovalute imaju relativno mnogo jedinica koncentriranih u rukama šačice pojedinaca (često kreatora i bliskih suradnika valuta). Ti imatelji učinkovito kontroliraju zalihe tih valuta čineći

ih osjetljivima na divlje promjene vrijednosti i izravne manipulacije - slično dionicama kojima se trguje. Međutim, čak i kriptovalute kojima se trguje široko podložne su volatilnosti cijena: vrijednost bitcoina udvostručila se nekoliko puta u 2017., a zatim prepolovila tijekom prvih nekoliko tjedana 2018. godine, da bi danas u svibnju 2021. prešla vrijednost od \$60.000 te se potom opet tek mjesec dana kasnije u lipnju gotovo prepolovila na \$32.000.

Problem kriptovaluta jest također što se često ne mogu zamijeniti za fiat valutu. Općenito, samo najpopularnije kriptovalute - one s najvećom tržišnom kapitalizacijom, izraženo u dolarima - imaju namjenske internetske burze koje dopuštaju izravnu zamjenu za fiat valutu. Ostale nemaju namjenske mrežne razmjene, pa se stoga ne mogu izravno zamijeniti za fiat valute. Umjesto toga, korisnici ih moraju pretvoriti u češće korištene kriptovalute, poput bitcoina ili ethereuma, prije fiat pretvorbe valuta. Povećavanjem troškova mjenjačkih transakcija, to suzbija potražnju, a time i vrijednost nekih manje korištenih kriptovaluta. Nadalje, iako rudari kriptovaluta služe kao kvaziposrednici za transakcije kriptovaluta, nisu odgovorni za arbitriranje sporova između strana u transakciji. Zapravo, koncept takvog arbitra krši decentralizacijski impuls u središtu moderne filozofije kriptovaluta. To znači da se pojedinac nema pravo žaliti ako je prevaren u transakciji - na primjer, unaprijedno plaćanje za stavku koja se nikada ne primi. Iako neke novije kriptovalute pokušavaju riješiti problem povrata sredstava, rješenja ostaju nepotpuna i uglavnom nedokazana. Suprotno tome, tradicionalni procesori plaćanja i mreže kreditnih kartica kao što su Visa, MasterCard i PayPal često se uključuju u rješavanje sporova između kupaca i prodavača. Njihova pravila povrata ili povrata sredstava posebno su osmišljena kako bi se spriječile prevare prodavača.

Naposljetku, velik problem čine i štetni utjecaji rudarstva kriptovaluta na okoliš. Rudarstvo kriptovaluta vrlo je energetske intenzivno. Najveći je „krivac“ bitcoin, najpopularnija svjetska kriptovaluta. Prema Martucciju (2017)²⁶ „*Prema procjenama koje navodi Ars Technica, rudarstvo bitcoina troši više električne energije nego cijela zemlja Danska.*“ Ipak kao kratkoročna i srednjoročna rješenja mogli bi se uzeti smanjivanje cijene bitcoina kako bi rudarstvo postalo manje unosno, potez koji bi vjerojatno trebao usklađeno miješanje u ono što je do sada bilo *laissez-faire* tržište, prelazak na algoritam kojemu je potrebno manje energije ili pak rezanje nagrade za rudarstvo brže od trenutno predviđene stope (prepolovljavanje svake četiri godine). Dugoročno gledano, najbolje rješenje jest napajanje rudnika kriptovaluta s niskim izvorima energije ili bez ugljika, možda uz popratne poticaje za premještanje rudnika u države s niskim udjelom ugljika poput Kostarike i Nizozemske.

²⁶ Martucci, B. (2017) *What Is Cryptocurrency – How It Works, History & Bitcoin Alternatives* [online]. Henderson: Money Crashers.

3. PODRUČJA I NAČIN PRIMJENE KRIPTOVALUTA

Tržište kriptovaluta segmentirano je na temelju tržišne kapitalizacije velikog broja kriptovaluta. Kriptovalute se preklapaju s ključnim područjima monetarnog i financijskog sustava. S obzirom na njihov brzi rast, složenost, veliku nestabilnost i potencijal za olakšavanje nezakonitih aktivnosti, njihovo uključivanje u postojeći sustav regulatorima i kreatorima politika širom svijeta predstavlja problem. Kao odraz povjerenja u pouzdanost i sigurnost blockchain tehnologije mnogi su predložili upotrebu blockchaina za upravljanje drugim aktivnostima poput glasanja, vladinih usluga, upravljanja identitetima ili trgovine u poljoprivredom sektoru. Te bi aktivnosti mogle izdavati vlastite kriptovalute. Kako je tehnologija još uvijek u nastajanju, izdavanje tih valuta ovisit će o razvoju usvajanja kriptovaluta i o tome kako će biti povezano s postojećim sustavima.

3.1. Temeljne kriptovalute prema tržišnoj kapitalizaciji

Procjena točne veličine tržišta može biti teška za bilo koju industriju, ali posebno za kriptovalute zbog velike volatilnosti cijena u kratkim vremenskim razdobljima. Od 1. prosinca 2017. ukupna tržišna kapitalizacija tržišta kriptovaluta iznosila je 326,7 milijardi dolara. Do 1. siječnja ove godine tržišna kapitalizacija kriptovaluta porasla je gotovo na 765,3 milijardi dolara, odnosno više se nego udvostručila. Prilikom pisanja ovog dijela diplomskog rada (23. lipnja 2021.) tržišna je kapitalizacija dosegla 1.349,9 milijardi dolara.

Grafikon 2. Ukupna tržišna kapitalizacija kriptovaluta od 1. srpnja 2017. do 1. lipnja 2021.



Izvor: <https://coinmarketcap.com/charts/> Pristupljeno: 23. lipnja 2021.

Postoji nekoliko pokretača koji su uzrok ovom golemom rastu tržišta kriptovaluta:

- 1) **Ekonomska ekspanzija** – Zanimarivši krizu uzrokovanu CoVidom-19, važan čimbenik u porastu tržišta kriptovaluta jest gospodarska ekspanzija. Naime, kako su se tržišni strahovi smirivali nakon recesije 2008. godine, apetit ulagača za rizikom vratio na razinu prije recesije, a kako je na tržište dionica 2017. doseglo gotovo rekordnu godinu, povjerenje investitora je poraslo te se stvorilo savršeno okruženje za rast nove vrste rizične imovine ulaganja.
- 2) **Blockchain tehnologija** - Blockchain je tehnološkim svijetom zavladao rastom bitcoina. Prije pojave blockchain tehnologije svijet kriptovaluta bio je gotovo bezvrijedan. Ova tehnologija ima duboke implikacije za mnoge industrije te je imala brze učinke na valutni i financijski svijet. Povećana učinkovitost, smanjeni transakcijski troškovi i povećana sigurnost koju blockchain pruža te stvaranje provjerljivih transakcija, istovremeno izbjegavajući digitalne naknade koje banke obično naplaćuju za transakcije, daju kriptovalutama gotovo svu vrijednost. Od uvođenja 2008. godine vrijednost kriptovaluta porasla je astronomskim stopama, a očekuje se da će se taj rast i integracija blockchaine u financijski sektor nastaviti.
- 3) **Investitorski apetit** - Jedno od glavnih pokretača rasta zabilježenog na kriptotržištu jednostavno je bilo veliko povećanje apetita investitora. Kriptovalute su dobile veliku pozornost investicijskih i državnih institucija koje su ih legitimirale kao investicijsku imovinu. Nadalje, Japan je izdao zakone koji zahtijevaju registraciju kriptovaluta kod agencija za financijske usluge - korak prema legalizaciji kriptovaluta. I krajem listopada 2017. CME je najavio da će započeti s izdavanjem derivata bitcoina. Svi ti događaji, između ostalog, pokazuju nagomilanu potražnju investitora za kriptovalutama.
- 4) **Atraktivne značajke ulaganja** - *Decentraliziranost*: Monetarna politika koju diktiraju središnje banke može uzrokovati devalvaciju centraliziranih valuta, dok kriptovalute ne kontrolira nijedna vlada i stoga nisu podložne volji središnjih banaka i kontroliraju se samo tržišnom dinamikom. *Sigurnost*: Kriptovalute su, po definiciji, sigurne. Decentralizirana priroda blockchain tehnologije omogućuje provjerljive transakcije na nekoliko geografskih lokacija, što smiruje strahove koje su kritičari u posljednjih deset godina izrazili u vezi s kriptovalutama. *Digitaliziranost*: budući da su kriptovalute potpuno virtualne, praktički ne postoje troškovi prijevoza niti transakcijski troškovi. Iako čak i internetske banke mogu naplaćivati naknade za transakcije, digitalna priroda kriptovaluta značajno smanjuje

troškove digitalnih transakcija. *Rast vrijednosti:* Porastom tehnologije koja je sposobna koristiti kriptovalute tržište je pokazalo da postoji velika želja za digitalnim valutama. Kao rezultat toga kriptovalute su postale vrijedna metoda za držanje i procjenu bogatstva.

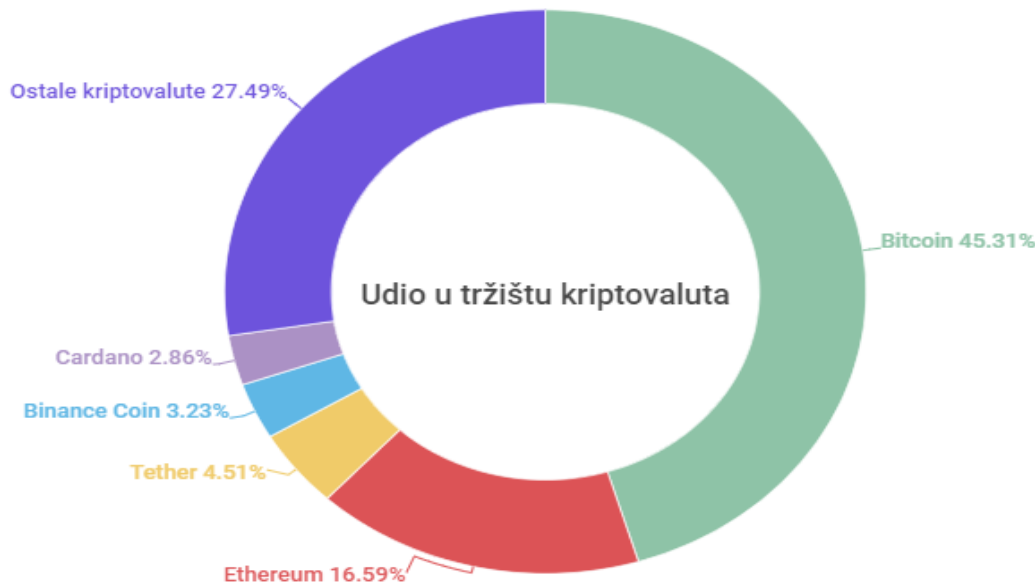
Najznačajnije kriptovalute prema tržišnoj kapitalizaciji prikazane su u tablici 1. i grafikonu 17.:

Tablica 1. Kriptovalute prema tržišnoj kapitalizaciji

Kriptovaluta	Tržišna kapitalizacija u \$ (cijena*količina u optjecaju)	Cijena u \$	Količina u optjecaju
 Bitcoin (BTC)	629,982,862,371	33,653.19	18,741,237
 Ethereum (ETH)	230,724,801,062	1,979.39	116,410,047
 Tether (USDT)	62,736,489,543	1.00	62,736,489,543
 Binance Coin (BNB)	44,948,283,087	293.04	153,432,897
 Cardano (ADA)	39,712,304,544	1.25	31,946,328,269

Izvor: izrada autorice prema podacima <https://coinmarketcap.com/>. Pristupljeno 23. lipnja 2021.

Grafikon 3. Udio u tržištu kriptovaluta u %



Izvor: izrada autorice prema podacima <https://coinmarketcap.com/>. Pristupljeno 23. lipnja 2021.

Na prethodnom grafikonu i tablici može se uočiti neosporna tržišna „dominacija“ bitcoina. Jedinstvena prednost bitcoina proizlazi iz činjenice da je to bila prva kriptovaluta koja se pojavila na tržištu. Bitcoin je uspio stvoriti globalnu zajednicu te potpuno novu industriju sastavljenu od milijuna pojedinaca koji stvaraju, investiraju, trguju i koriste bitcoin i druge

kriptovalute u svom svakodnevnom životu. Pojava prve kriptovalute stvorila je konceptualnu i tehnološku osnovu koja je nakon toga nadahnula razvoj tisuću konkurentskih projekata. Čitavo tržište kriptovaluta temelji se na ideji koju je realizirao bitcoin: novac koji može poslati i primiti bilo tko, bilo gdje u svijetu bez oslanjanja na pouzdane posrednike poput banaka i tvrtki za financijske usluge. Prednost velikim dijelom duguje i sveprisutnosti platformi koje pružaju razne usluge: novčanike, razmjene, usluge plaćanja, internetske igre i još mnogo toga. Danas prema *CoinMarketCapu*²⁷ na tržištu postoji više od 10.600 vrsta kriptovaluta. Međutim, ovdje valja istaknuti kako to nisu iste vrste kriptovaluta te treba napraviti distinkciju među kriptovalutama, altcoinima te digitalnim tokenima.

3.1.1. Kriptovalute, altcoini i digitalni tokeni

Kriptovaluta vs. altcoin

Kriptovaluta je standardna valuta koja se koristi za izvršavanje ili primanje plaćanja na blockchainu, a najpopularnija je kriptovaluta bitcoin. Altcoini su razne kriptovalute koje su pokrenute nakon masovnog uspjeha koji je postigao bitcoin. Zamišljene su kao poboljšane zamjene bitcoina. Litecoin, dash, monero i ripple samo su neki primjeri altcoina. Općenito govoreći, altcoini djeluju slično kao i originalni bitcoin. Pomoću privatnog ključa šalje se uplata iz digitalnog novčanika jednog u novčanik drugog korisnika. I kod ovih kriptovaluta postoji blockchain gdje se transakcije trajno i javno bilježe, pa se razmjene ne mogu mijenjati. Ipak, altcoini ne slijede sva ista pravila kao i bitcoin.

Primjerice, dok blockchain bitcoina proizvodi bitcoine svakih 10 minuta, altcoin litecoin proizvodi kovanice svake 2,5 minute, što omogućuje litecoinu mogućnost brže obrade plaćanja. Litecoinov blockchain također će proizvesti 84 milijuna litecoina, dok će bitcoinov proizvesti samo 21 milijun bitcoina²⁸. Isto tako, litecoin koristi drugačiji skup pravila za rudarstvo od bitcoina. Dok bitcoin zahtijeva skupi hardver za rudarenje, litecoin se može rudariti uobičajenim računalnim hardverom. Nadalje, altcoini često mijenjaju pravila bitcoina dovoljno da proizvedu nešto jedinstveno s određenom primjenom.

Neki altcoini poput solarcoina²⁹ zamišljeni su kao mjenjačnica za proizvodnju solarne energije. Drugi poput namecoina³⁰ stvorili su osnovu za novi sustav naziva domena na Internetu, dok su

²⁷Internetska stranica koja prikuplja i izvještava o aktivnostima koje se događaju na tržištu kriptovaluta, ali izravno ne prodaje nijednu kriptovalutu.

²⁸ <https://litecoin.org/>

²⁹ <https://solarcoin.org/>

³⁰ <https://www.namecoin.org/>

stablecoini altcoini dizajnirani za borbu protiv volatilnosti kriptovaluta vezujući njihovu vrijednost za valutu, indeks, robu ili vrijednosni papir. Primjeri stablecoina su tether i libra koju je razvio Facebook. S jedne strane, altcoini su općenito dizajnirani za rješavanje uočenih nedostataka bitcoina, bilo da se radi o brzini, troškovima rudarenja ili nekom drugom čimbeniku. S druge strane, kao vrsta ulaganja, altcoini su vrlo novi i njihova se vrijednost može drastično promijeniti te su, kao i bitcoin, često predmet prevara.

Kriptovaluta vs. digitalni token

U osnovi kriptovalute i altcoini imaju svoj vlastiti blockchain i prvenstveno se koriste kao medij za digitalna plaćanja, kao skladište vrijednosti ili kao obračunska jedinica. S druge strane, tokeni se stvaraju na postojećim blockchainima. Zapravo, zahvaljujući stvaranju i olakšavanju pametnih ugovora najčešća platforma blockchain tokena jest ethereum. Tokeni koji su izgrađeni na ethereum platformi poznati su kao ERC-20 tokeni, a obično se distribuiraju, prodaju i cirkuliraju kroz standardni postupak ICO-a koji uključuje grupno financiranje za financiranje razvoja projekta. Ako se token kreira na ethereumu, kreator mora potrošiti dio ethereuma da bi rudari mreže potvrdili transakciju (stvaranje) tokena. Važno je imati na umu da naknade treba platiti za sve transakcije tokena na blockchainu, a ne samo za izradu tokena. Stoga bilo koja aplikacija izgrađena na ethereumu mora koristiti ethereum kovanice za prijenos tokena specifičnih za aplikaciju s jednog korisnika na drugog ili između aplikacije i korisnika.

Većina tokena postoji za upotrebu s decentraliziranim aplikacijama ili *dApps*. Kada programeri kreiraju svoj token, oni mogu odlučiti koliko jedinica žele izraditi i gdje će ti novi tokeni biti poslani kada se kreiraju. Oni će platiti dio izvorne kriptovalute na blockchainu na kojem trenutno stvaraju token. Jednom stvoreni, tokeni se često koriste za aktiviranje značajki aplikacije za koju su dizajnirani. Na primjer, Musicoin³¹ je token koji korisnicima omogućuje pristup različitim značajkama Musicoin platforme poput gledanja glazbenog videozapisa ili puštanja pjesme. Binance mjenjačnica također ima svoj token. Kada korisnici trguju s ovim tokenom, naknade su im 50% manje.

Neki su tokeni stvoreni da predstavljaju fizičku stvar. WePower (WPR)³² dobar je primjer tokena koji predstavlja fizičku stvar. Projekt WePower omogućava korisnicima kupnju i prodaju električne energije na blockchainu pomoću pametnih ugovora. Njegov token (WPR) predstavlja određenu količinu energije. Dobar primjer je i Civic³³ koji koristi token CVC.

³¹ <https://musicoin.org/>

³² <https://wepower.com/>

³³ <https://www.civic.com/>

Njegova aplikacija prati šifrirane identitete na ethereum blockchainu. Cilj mu je pružiti jeftiniji, pouzdaniji i učinkovitiji način provjere identiteta. Svaka tvrtka ili organizacija koja upotrebljava digitalni identitet može provjeriti valjanost podataka pomoću blockchaina. Što se više puta aplikacija koristi, to više povjerenja imaju treće strane u digitalni identitet pohranjen u Civicu. Na primjer, za inozemno putovanje potrebno je potvrditi svoj identitet zrakoplovnoj tvrtki. Ako je zrakoplovna tvrtka bila partner tvrtke Civic, šalje se QR kôd koji traži podatke o putniku. Pomoću aplikacije Civic podatci se šalju izravno tvrtki s mobilnog uređaja. Podaci su pohranjeni na uređaju, ali su u potpunosti šifriranim, što sprječava krađu. Skeniranje otiska prsta ili šarenice može dokazati da ste vlasnik primljenih podataka.

Budući da programer dApp-a i tokena ne mora stvoriti vlastiti blockchain, to štedi vrijeme i resurse. Oni mogu koristiti značajke kriptovalute sa svojom aplikacijom, a istovremeno imaju koristi od sigurnosti i rudara izvornog blockchaina. Potrebno je puno rudara da bi stvorili snažan blockchain koji se ne može napasti. Mnogo je logičnije da mnoga računala rade na jednom zajedničkom blockchainu na kojem može raditi nekoliko aplikacija, umjesto da postoje tisuće slabih, uglavnom centraliziranih blockchaina.

Konačno, može se izdvojiti još nekoliko vrsta tokena: *security tokeni* čijom kupovinom osoba koja ih kupuje ulaže svoj novac u ICO s očekivanjem dobiti (s njima se postupa na isti način kao i s tradicionalnim vrijednosnim papirima), *kapitalni tokeni* koji predstavljaju neku dionicu ili kapital u tvrtki koja ga izdaje, *utility tokeni* ili aplikacijski tokeni koriste se kako bi ljudima omogućili pristup bilo proizvodu ili usluzi te *tokeni plaćanja* koji se koriste samo za plaćanja robe i usluga.

3.1.2. Burze kriptovaluta

Burza kriptovaluta ili digitalna burza (DCE) omogućava kupcima da trguju kriptovalutama za drugu imovinu poput fiat novca ili drugih digitalnih valuta. Ove burze mogu prihvaćati plaćanja kreditnim karticama, devizne doznake ili druge oblike plaćanja u zamjenu za kriptovalute. Burza kriptovaluta može biti *market maker* koji obično koristi *bid-ask* raspon kao proviziju za uslugu ili jednostavno naplaćuje naknade. Prema Conwayu³⁴ ovo su najznačajnije kriptoburze:

Coinbase

Coinbase, najkorištenija burza kriptovaluta, osnovana je 2012. godine te je potpuno regulirana i licencirana burza kriptovaluta. Nudi izuzetno jednostavnu razmjenu koja u velikoj

³⁴ Conway, L. (2021) *Best Crypto Exchanges* [online]. New York: Investopedia.

mjeri smanjuje prepreku u ulaganje u kriptovalute, što se obično smatra zbunjujućim i zamršenim. Coinbase također nudi osigurane skrbničke novčanike za ulagače i trgovce da čuvaju svoja ulaganja. Ovi skrbnički računi vrlo su prikladni za novije korisnike, no privatni ključevi valuta u njima u vlasništvu su Coinbasea, a ne investitora. Uz to, Coinbase također nudi besplatnu verziju CoinbasePro koja ima drugačiju, ali jeftiniju strukturu naknada i znatno više opcija u pogledu grafikona i pokazatelja. CoinbasePro savršen je sljedeći korak za one koji su ovladali Coinbaseom, a pomaže zaokružiti cjelokupnu ponudu dodavanjem značajki koje bi napredniji korisnik želio. Naknada za transakcije iznosi između 0,99 i 2,99 dolara, ovisno o vrijednosti kupnje.

Binance

Burza Binance osnovana je 2017. godine s fokusom na trgovanje altcoinima. Binance nudi preko 100 različitih trgovinskih parova između različitih kriptovaluta te nekoliko fiat-kripto parova, premda je većina parova između kriptovaluta. Trenutno Binance čini najznačajniji dio količine kriptotrgovalja dnevno. Burza trenutno ne dopušta depozite u američkim dolarima, ali omogućuje izravnu kupnju odabranog broja kriptovaluta kreditnom ili debitnom karticom. Dopušteni su depoziti koji koriste preko 20 drugih fiat valuta, uključujući euro. Binance je najprikladniji za pojedince koji bi željeli trgovati ili ulagati u manje poznate altcoine. Na primjer, Coinbase nudi samo 22 različite kriptovalute za trgovanje, dok Binance ima preko 50. Binance je idealan za sve koji žele trgovati altcoinima ili one koji žele naprednije grafike od većine drugih burzi. Korištenje Binanceove matične kriptovalute, BNB, snižava naknade za 25%.

Bisq

Bisq je softver za preuzimanje, ali ujedno i kriptoburza. Na Bisqu nitko osim korisnika ne kontrolira njegova sredstva, čime se razlikuje od centralizirane razmjene koja kontrolira korisnikova sredstva na skrbničkom računu na kojem korisnik nema privatne ključeve. U tom scenariju Coinbase zadržava pravo zaplijeniti korisnikova sredstva ako aktivnost njegova računa smatra sumnjivom bez obzira je li ta aktivnost zapravo legalna. Bisq je odmah dostupan svima koji imaju računalo ili pametni telefon jer ne postoji postupak registracije ili pravilo KYC (engl. *know-your-customer*). Kako na svijetu postoje milijuni ljudi koji nemaju pristup sredstvima za trgovanje jer njihove države možda nemaju odgovarajuću financijsku infrastrukturu, ovo ga čini idealnim za one koji traže privatnost ili za pojedince nemaju nikakve državne isprave. Bisq nudi trgovinu s nekoliko različitih fiat valuta, uključujući dolar, kao i

bitcoin i niz drugih kriptovaluta. Njegove decentralizirane i peer-to-peer karakteristike mogu značiti nizak opseg trgovine i sporije transakcije, ali nekima se to i te kako isplati. Naknade za trgovanje plaćaju se u BTC ili BSQ (izvorna kriptovaluta mjenjačnice).

Cash App

Cash App je peer-to-peer sustav prijenosa novca. Ova vrsta usluge omogućuje korisnicima dijeljenje hrane, plaćanje stanarine ili čak kupovinu na mreži kod trgovca koji podržava Cash App. Cash App u osnovi može djelovati kao bankovni račun, a korisnici mogu imati vlastite debitne kartice Cash App. Cash App također omogućuje svojim korisnicima ulaganje u dionice, ETF-ove i kriptovalute. Sučelje za mobilne uređaje koje koristi ova burza vrlo je jednostavno shvatiti i koristiti, što ga čini idealnim za početnike koji ulažu. Isto tako, Cash App omogućuje korisniku da povuče ulaganja u kriptovalute u vlastiti novčanik, što je izuzetno važno u kriptozajednici. Cash App naplaćuje naknadu za uslugu za svaku transakciju. Također naplaćuje naknadu određenu volatilnošću cijena. Te se naknade mijenjaju ovisno o aktivnosti tržišta. Glavni je nedostatak što trenutno dopušta samo ulaganje u bitcoin te što postoji ograničenje povlačenja bitcoina u vrijednosti od 2.000 USD svaka 24 sata.

3.2. Svakodnevna upotreba kriptovaluta

Kriptovalute nisu iskoristive samo u financijskom svijetu već se sve više počinju upotrebljavati i u svakodnevnom životu. Kako se svaki dan odvija preko tisuću kriptotransakcija, jasno je da već postoji značajna baza korisnika kriptovaluta. Ova baza korisnika može poslužiti kao temelj za uvođenje ove revolucionarne tehnologije u naš svakodnevni život, posebno jer primjene kriptovaluta izvan kriptoburzi postaju sve očitije. Prelazak s pomalo izoliranog alata za trgovanje na funkcionalnu valutu sljedeći je veliki korak za kriptosvijet. Iako ovo može zvučati kao razvoj u dalekoj budućnosti, kriptovalute već danas donose brojne prednosti.

Primjerice, postoji pregršt usluga koje nude debitne kartice za kriptovalute koje se podižu izravno s kriptoračuna premda se obično može pristupiti samo nekoliko glavnih kriptovaluta. Svaka valuta ima svoje račune pohranjene na blockchainu sa saldima i pristupnim kodovima kojima se može pristupiti izravno iz telefonske aplikacije. Postoje specijalizirane aplikacije (npr. Exodus i Jaxx) koje olakšavaju plaćanje transakcija skenirajući QR kod telefonom. Nadalje, španjolska banka Santander kreirala je internetsku uslugu koja građanima omogućuje plaćanje računa internetom, čime su željeli uključiti i kriptovalute u ovaj proces. Usluga prihvaća uplatu korisnika i pretvara ju u kriptovalutu koja se zatim može koristiti za plaćanje

računa. Preko 45.000 tvrtki registrirano je na [billpayforcoins.com](https://www.billpayforcoins.com)³⁵ kako bi prihvatili neki oblik kriptovalute kao plaćanje računa za električnu energiju, računa za plin, računa osiguranja itd. Stvari također olakšavaju i internetske stranice poput [coinatmradar](https://coinatmradar.com/)³⁶ koji pomaže naći automate u blizini korisnika za kupovinu ili prodaju kriptovaluta ili pak [coinmap](https://coinmap.org/)³⁷ koji pokazuje mjesta na kojima se prihvaća plaćanje kriptovalutama.

U Europi je stvorena inovativna platforma za plaćanje karticama [tap](https://www.tap.global/)³⁸ koji donosi izravniji način kako koristiti kriptovalutu u svakodnevnom životu. Platforma olakšava svakome tko drži kriptovalutu da je izravno troši ili trguje njome u najkraćem mogućem intervalu. Platforma osigurava likvidnost po najpovoljnijoj cijeni za kupce jednostavnim postupkom identifikacije, provjera je valjanosti brza te se uklanjaju transakcijske barijere koje već postoje među kriptoposjednicima. U SAD-u je pak osnovan [BitPay](https://bitpay.com/)³⁹ s ciljem da poslovnim subjektima olakša prihvaćanje bitcoina kao opcije plaćanja, a nastavio je širiti svoje usluge u različitim dijelovima svijeta.

Istraživanje HSB-a za 2020. godinu⁴⁰ otkrilo je da 36% malih i srednjih tvrtki u SAD-u prihvaća bitcoin ili drugu kriptovalutu. Tvrtke dolaze iz raznoraznih gospodarskih područja. Tako Wikimedia, tvrtka koja upravlja najvećom svjetskom *open-source* enciklopedijom Wikipedijom, prihvaća donacije⁴¹ u bitcoinu, a plaćanje se obavlja na platformi BitPay. Tvrtka Microsoft dopušta upotrebu bitcoina za nadogradnju računa i usluga⁴². AT&T⁴³ je prvi veliki američki mobilni operater koji pruža mogućnost plaćanja kriptovalutama kupcima putem BitPaya. U industriji brze prehrane ističe se KFC Kanada⁴⁴ koji je odlučio prihvatiti bitcoin u zamjenu za kanticu pržene piletine, tzv. „bitcoin bucket“. Tvrtka obrađuje plaćanje BitPayom i kantica se isporučuje izravno na kućnu adresu kupca.

Zatim, prema lokalnim vijestima prodajna mjesta Burger Kinga u Venezueli⁴⁵ najavila su partnerstvo s Cryptobuyerom radi prihvaćanja kriptovaluta kao načina plaćanja. Kupci mogu

³⁵ <https://www.billpayforcoins.com/index.php>

³⁶ <https://coinatmradar.com/>

³⁷ <https://coinmap.org/>

³⁸ <https://www.tap.global/>

³⁹ <https://bitpay.com/>

⁴⁰ Milewski, D. (2020) *HSB Survey Finds One-Third of Small Businesses Accept Cryptocurrency: Do They Understand the Cyber and Financial Risks?* [online], San Francisco: Business Wire.xType equation here.

⁴¹ Web-stranica dostupna je na sljedećoj poveznici: https://donate.wikimedia.org/wiki/Ways_to_Give

⁴² BBC News – službena stranica (2014). *Microsoft to accept payments made in bitcoins* [online]. London.

⁴³ AT&T – službena stranica (2019). *AT&T is the First Mobile Carrier to Accept Payment in Cryptocurrency* [online]. Dallas

⁴⁴ Higgins, S. (2018) *KFC Canada Is Accepting Bitcoin for Fried Chicken* [online]. New York Francisco: CoinDesk.

⁴⁵ La Patilla – službena stranica (2020). *Burger King Venezuela abre las puertas a las criptomonedas* [online]. Caracas.

plaćati bitcoinom, dashom, litecoinom, ethereumom i tetherom. Usto, njemačka podružnica Burger Kinga⁴⁶ počela je prihvaćati bitcoin na svojoj web-stranici i u mobilnoj aplikaciji 3. rujna 2019. Bitcoinima i bitcoin cashom može se platiti dostava putem dostavne službe Lieferservice koja radi s restoranima u cijeloj zemlji.

U svijetu sporta klub američkog nogometa Miami Dolphins⁴⁷ namjerava gledateljima utakmica pružiti mogućnost plaćanja litecoinom i bitcoinom prilikom kupnje ulaznica, pri čemu se polovica prihoda izdvaja za dobrotvorne ciljeve kluba. Košarkaški klub Dallas Mavericks⁴⁸ prihvaća bitcoin kao način plaćanja i za ulaznice za igru i za robu. BitPay će obrađivati sva Bitcoin plaćanja putem internetske stranice tima.

Internetska stranica digitalnih sadržaja zabavnih medija i softvera The Pirate Bay prihvaća donacije bitcoina i kriptovaluta od 2013. godine. Neprofitna digitalna knjižnica The Internet Archive⁴⁹ s navedenom misijom „univerzalnog pristupa svim znanjima“ prihvaća donacije bitcoina. Iako Amazon⁵⁰, kao najveći internetski trgovac danas, ne prihvaća izravno bitcoin, pomoću stranice Purse.io moguće je kupiti bilo što na web-mjestu i platiti bitcoinom. Purse.io povezuje ljude koji imaju bitcoin i žele kupiti na Amazonu s ljudima koji žele dobiti bitcoin zauzvrat za ispunjavanje narudžbe. Osim navedenih treba još spomenuti i tvrtke poput Pizza Huta, Subwaya, ExpressVPN-a, CheapAira, Norwegian Aira, Twitcha i ostale.

3.3. Primjeri zemalja koje uvode digitalne valute središnjih banaka

Tijekom godina tradicionalna bankarska regulatorna tijela širom svijeta borila su se za kontrolu rastućeg utjecaja popularnih kriptovaluta poput bitcoina i ethereuma koji rade na blockchain mreži. Ove kriptovalute stekle su golemu popularnost zahvaljujući svojoj decentraliziranoj prirodi i nedostatka regulacije, a postale su prijetnja današnjem tradicionalnom bankarskom sustavu koji djeluje pod nadzorom regulatornog tijela neke države poput središnje banke. Usto, kontinuirano lansiranje novih kriptovaluta potaklo je i zabrinutost zbog mogućnosti prijevara, krađa i hakiranja. Kako je bitcoin dobivao na važnosti u javnoj domeni, bolje razumijevanje tehnologije koja je stajala iza njega olakšalo je ljudima stvaranje alternativnih kriptovaluta tzv. altcoins koji uključuju kovanice stvorene za specifične svrhe ili određene demografske skupine,

⁴⁶ Magas, J. (2019) *Bitcoin Not Accepted: Burger King's Crypto Foray Short-Lived* [online]. New York: Cointelegraph.

⁴⁷ Miami Dolphins – službena stranica (2019). *Litecoin Named Official Cryptocurrency of the Miami Dolphins* [online].

⁴⁸ Rader, D. (2019) *The Dallas Mavericks Are Now Accepting Bitcoin* [online]. New York: Forbes.

⁴⁹ <https://archive.org/donate/cryptocurrency/>

⁵⁰ <https://purse.io/shop>

kao što je Permacredits, vrsta kriptovalute kojoj je cilj biti uspostavljena trgovinska valuta za održive poljoprivredne tvrtke. Ne mogavši kontrolirati rast i utjecaj takvih kriptovaluta, mnoge vodeće središnje banke širom svijeta rade ili razmišljaju o pokretanju vlastitih verzija kriptovaluta. Te se regulirane kriptovalute nazivaju digitalne valute središnje banke (engl. *Central Bank Digital Currency*), a njima bi upravljale odgovarajuće monetarne vlasti ili središnje banke određene zemlje. CBDC bi trebale djelovati kao digitalni prikaz fiat valute neke zemlje, a bile bi podržane odgovarajućom količinom monetarnih rezervi poput zlata ili deviznih rezervi.

3.3.1. Digitalne valute čija upotreba nije sasvim zaživjela

Države s različitih kontinenata nastojale su uvesti i ubrzati usvajanje vlastitih digitalnih valuta kako bi ispunile svoje različite ciljeve.⁵¹ Zanimljivo je da mnoge od ovih valuta dolaze iz eurozone, a mogu se podijeliti u dvije glavne kategorije. Primjerice, kriptovalute ekonomija poput Portugala i njegovog CryptoEscuda te Grčke i njezinog GreeceCoina, koje su teško podnijele krizu 2008. godine, imaju za cilj „popraviti“ gospodarstvo i pružiti održivu alternativu za jačanje gospodarstva. S druge strane, druga kategorija kriptovaluta eurozone jesu kriptovalute temeljene na suverenitetu i nacionalizmu, npr. njemačka eMark ili nizozemski eGulden. Imena ovih valuta posuđena su od prijašnjih valuta korištenih do prihvaćanja eura 2002. godine. S obzirom na dobrostojeća gospodarstva ovih zemalja one bi kriptovalute uvele tek kao alternativu postojećem financijskom sustavu. Bez obzira na to jesu li potaknute lošom ekonomijom ili „nostalgijom“, većina ovih valuta dijeli zajednički obrazac: iza sebe nemaju nikakav sveobuhvatan ekonomski dizajn ili planiranje. Uglavnom su to jednostavni klonovi litecoina, s crtom nacionalizma te u njih nije uloženo puno planiranja i promišljanja, što nažalost ozbiljno ograničava njihovu korisnost i potencijal za rast.

AuroraCoin – Island

AuroraCoin je vjerojatno najpoznatiji nacionalni altcoin do danas. Promoviran je da se islandskim građanima ponudi mogućnost konsolidacije bogatstva jer država ima strogu kontrolu kapitala u pogledu pretvorbe bogatstva kako bi spriječila pretjerani odljev. U osnovi je dizajniran za obnovu ekonomskih mostova između Islanda i ostatka svijeta koristeći tehnologiju kriptovaluta. Nakon početnog vrhunca cijena nedugo nakon objavljivanja, gdje je

⁵¹ Kuo Chuen, D. L. (2015.) *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Amsterdam: Elsevier Inc., str. 67-80.

u jednoj fazi to bila kriptovaluta s trećom najvećom tržišnom kapitalizacijom, vrijednost AuroraCoina drastično je pala, što se može pripisati raznim čimbenicima, a često se navodi i nedostatak znanja i svijesti među građanima. Na primjer, nije bilo trgovaca koji su se prijavili za prihvaćanje kovanica te jedino što su građani Islanda mogli učiniti s kovanicama bilo je okrenuti se i prodati ih za bitcoin. I upravo se to dogodilo. Ove su kombinacije uzrokovale dramatičan pad cijene. Budući da su rudari „odlazili“, transakcije su se obrađivale jako sporo. Dvanaestosatna vremena potvrde nisu bila neobična, što je dodatno pomoglo srušiti cijenu i pridonijeti silaznoj spirali.

SpainCoin i PesetaCoin – Španjolska

SpainCoin pokazao je sve znakove plemenitog i neuspjelog pokušaja u dizajniranju nacionalne kriptovalute s obzirom na to da je učinjeno vrlo malo da se osigura da valuta ostane u optjecaju i za održavanje razine upotrebe. Valuta je izdana s tim da je 50% dodijeljeno ljudima koji nemaju pristup ili čak ni ne znaju ništa o kriptovalutama kako bi ih se potaknulo da ih koriste. Početna cijena nevjerojatno je porasla, a zatim se brzo srušila i pokrenula dugu, ravnu krivulju cijena koja se približavala nuli. PesetaCoin je prva kriptovaluta stvorena za Španjolsku prije SpainCoina. Objavljena je s planom da njezino usvajanje bude postupno. Nepotrebno natjecanje sa SpainCoinom, međutim, kočilo je njegov napredak.

AphroditeCoin – Cipar

Nakon financijske krize mnogi su stanovnici Cipra pokušavali kupiti bitcoin kao sredstvo zaštite vlastite uštedevine protiv nestabilnosti matične valute. AphroditeCoin pušten je pod pseudonimom "Costa Themistocleus", bez dodatnih detalja. Mnogi su promatrači od početka ispitivali legitimitet AphroditeCoina s obzirom na nedostatak informacija i izrazitu volatilnost tržišnih cijena.

GaelCoin i IrishCoin – Irska

GaelCoin prva je od dvije irske kriptovalute, a također se prodavao kao mjera za ponovno pokretanje gospodarstva. Njegov web-portal među najnovijim je i najinformativnijim, a vijesti i tehnički detalji dostupni su svim vlasnicima valuta ili rudarima. Za IrishCoin pak nema dovoljno dostupnih podataka jer se ne dobiva tradicionalnim metodama rudarenja, umjesto toga, zamišljen je kao alat koji pomaže promociji turističkog sektora u Irskoj. Stoga bi valutu uveli trgovci, djelujući ili kao bon za popust ili kao doznaka.

MapleCoin - Kanada

MapleCoin je nacionalna kriptovaluta Kanade i trebao je biti svojevrsni sef za nacionalne financije, radi očuvanja bogatstva Kanade. To znači da je projicirana kao virtualna roba slična zlatu, a ne kao valuta za zamjenu. Korisnike se poticalo da ih prikupljaju i drže te da ih koriste za zaštitu od vanjskih uvjeta za fiat valute. Međutim, to znači da s malo ili nimalo MapleCoina u optjecaju ne postoji način utvrditi koja je fer-vrijednost valute.

IsraCoin – Izrael

Programeri IsraCoina nadali su se da će uvođenje kriptovalute poremetiti uspostavljeni bankarski sustav kako bi se bogatstvo decentraliziralo, stvarajući jednake uvjete za sve. Na prvi pogled Izrael se čini idealnim kandidatom za brzo uvođenje nacionalne kriptovalute s visokom razinom tehnologije. Međutim, prihvaćanje valute među stanovništvom u najboljem slučaju bilo je mlako te je potrebno više vremena prije nego što se pravilno asimilira u izraelsko gospodarstvo.

3.3.2. Digitalne valute na čijem se uvođenju aktivo radi

Da bi bilo koji oblik novca mogao funkcionirati, mora se smatrati dovoljno održivim kao sredstvo razmjene, obračunskom jedinicom i zalihom vrijednosti, a u mnogim slučajevima primjena kriptovaluta nije uspjela izvršiti nijedno od spomenutog uspješno. Primjetni propusti koji su zajednički nekim od ovih valuta bili su poremećaji u plaćanjima koji su smatrani poticajem šire ekonomske krize, a način plaćanja postao je značajan sistemski rizik kako na domaćem tako i na međunarodnom nivou. Te manjkavosti karakteristične za kriptovalute trebala bi riješiti digitalna valuta izdana od strane središnje banke ili drugi alternativni oblici digitalne valute izdane u reguliranom sustavu. Srećom, postoje primjeri koji su postigli određeni stupanj uspjeha, a čije će se karakteristike objasniti dalje u tekstu.

e-Krona - Švedska

Švedska je jedna od zemalja koja se kreće u smjeru društva bez gotovine. Švedska središnja banka Riksbank smatra da bi nova valuta e-Krona trebala biti ekvivalentna redovnoj valuti zemlje, ali da se koristi za male transakcije između potrošača, tvrtki i vlasti. Središnja banka odlučila je za projekt koristiti IOTA-in blockchain, poznat i kao Tangle. Njegova posebnost leži u tome što nema blokove, lance ili rudare. Na taj način sudionici moraju aktivno sudjelovati u konsenzusu mreže ako žele obavljati transakcije. Također, kako Švedska nije u eurozoni, pri

izdavanju valute neće postojati sukob interesa s Europskom središnjom bankom (ECB).

J-coin - Japan

Otpriblike polovica od oko 100 regionalnih banaka u Japanu predstaviti će novi sustav bezgotovinskog plaćanja koji je razvila Mizuho Financial Group Inc. Ovo je bio pokušaj japanske vlade da proširi upotrebu bezgotovinskog plaćanja uoči Olimpijskih igara u Tokiju 2020. godine. J-Coin trebao bi nadopuniti japanski jen i bit će vezan za nj na način 1:1 putem kojeg će građani moći kupiti robu i usluge, a transakcije će se obrađivati aplikacijom za pametne telefone koristeći dvodimenzionalni crtični kôd "Quick Response".

CryptoRuble - Rusija

Vladimir Putin u listopadu 2017. godine najavio je da će Rusija izdavati vlastitu valutu CryptoRuble koju će financirati država. Valuta se neće rudariti, već će je izdavati vlada. U biti, valuta će predstavljati rublju, ali digitalnu i šifriranu. CryptoRuble će imati istu cijenu kao i rublja te će biti zamjenjiva za tradicionalne rublje. Kako je sam Predsjednik izjavio da su se kriptovalute uglavnom koriste za kriminal, glavnim razlogom izdavanja smatra se stopiranje prometa ostalih kriptovaluta.

emCash - Ujedinjeni Arapski Emirati

Nakon uspješnog pothvata emWalleets od 2017. vlada Dubaija radi na blockchain tehnologiji, tj. emCash valuti za digitalne transakcije održavajući anonimnost, što pruža mogućnost ravnopravne transakcije bez otkrivanja identiteta osoba koje su uključene u transakciju. emCash dolazi s emPayom, odnosno mobilnim novčanikom. Njihova najveća prednost jest što će transakcije biti izvršene u kratkom roku na siguran način. Moći će se koristiti za uobičajene transakcije poput kupovanja filmova, plaćanja računa, prehrane, školarina, namirnica, razonode itd.

Petro - Venezuela

Venezuela je lansirala vlastitu nacionalnu kriptovalutu petro u veljači 2018. Venezuelanska vlast tvrdi da je petro podržan rezervama nafte i minerala u zemlji te bi vrijednost 1 petra trebala biti jednaka cijeni 1 barela nafte, a namijenjen je nadopunjivanju strelovito padajuće valute bolívar fuerte. Venezuelanska vlada također namjerava koristiti petro kao sredstvo za zaobilazanje američkih sankcija i pristup međunarodnom financiranju.

Digital Yuan - Kina

YuanPay grupa započela je razvoj kineske nacionalne kriptovalute 2014. Dosada je YuanPay jedina legalizirana tvrtka u Kini koja trguje i prodaje kriptovalute s obzirom na to da je Kina od rujna 2017. najavila zabranu prodaje ili razmjene bilo kojeg ICO-a ili kriptovalute, čak je i razmjena suprotna zakonu. Za razliku od drugih kriptovaluta digitalni yuan strogo će kontrolirati kineska vlada. Dakle, izostat će prednosti poput decentralizacije i anonimnosti. Ipak, uzevši u obzir da Kina ima najveći broj ljudi koji nemaju pristup banci, digitalna valuta omogućit će većem broju njih da sudjeluju u gospodarstvu bez skupih bankarskih proizvoda i infrastrukture.

Od ostalih država treba spomenuti Ekvador koji 2015. godine uveo sustav pod imenom dinero electrónico s ciljem da ne bude direktno vezan za američki dolar. Zatim, Senegal sa svojom valutom akoin nazvanom po popularnom pjevaču Akonu koji je investirao u izgradnju pametnog grada u blizini glavnog grada Dakara, čija će temeljna valuta biti upravo akoin. Ostale države koje aktivno rade na uvođenju ovih valuta ili tek razmišljaju o njihovom uvođenju uključuju SAD, Ujedinjeno Kraljevstvo, Indiju, Tunis, Estoniju, Singapur i Australiju. Spomenute digitalne valute, distribuirane, elastične i zasnovane na blockchainu, mogu pomoći da nacionalna trgovina i međunarodna trgovina postanu bez trenja. One mogu pojednostaviti ili automatizirati oporezivanje i pomoći u borbi protiv korupcije, pružiti platformu za provjeru vlasničkih prava, integrirati ljude s niskim primanjima i stvoriti vrijednost i radna mjesta. Ako se pravilno koriste, nacionalne kriptovalute postat će novi val budućnosti. Međutim, da bi nacionalna kriptovaluta imala bilo kakav utjecaj, potrebno je puno više od entuzijazma i tehnologije. Ispravno dizajnirane novčane značajke, podrška za trgovce, integracija POS-a, integracija bankomata, marketing i poslovni odnosi moraju biti dio plana. Tek kada se sve navedeno izvrši pravilno, tada se može ostvariti puni potencijal nacionalne kriptovalute.

3.4. Temeljni pokazatelji vrijednosti kriptovaluta pri kriptotrgovanju

Predvidjeti u kojem će se smjeru kretati cijena kriptovaluta nije lako i zato postoje pokazatelji. Pokazatelji kriptovaluta alati su u kombinaciji s tehničkom analizom koji trgovateljima mogu pomoći u predviđanju kretanja cijena kriptovaluta s većom točnošću. Tehnička analiza oslanja se na povijesne podatke kako bi pružila matematičke modele vjerojatnog djelovanja cijena, a ti su modeli pretvoreni u pokazatelje. Podaci iz formula zatim se crtaju na grafikonu, a potom se postavljaju na grafikon trgovanja pomažući trgovateljima u donošenju odluka. Iako pokazatelji

kriptovaluta ne mogu predvidjeti kretanje cijena sa 100%-tnom preciznošću, njihovo opravdanje proizlazi iz činjenice da kretanje cijena ima zamah, a što više impulsa cijena vidimo u određenom smjeru, teže ga je zaustaviti. Stoga se pokazatelji koriste grafikonima i formulama kako bi dobili jasniju sliku o tome što će kupac i prodavatelj vjerojatno sljedeće učiniti. Tehnička analiza ima za cilj identificirati mogućnosti trgovanja iskorištavanjem trendova cijena i obrazaca koji proizlaze iz vremenskih serija kriptovaluta.

U stvari, mnogi se trgovatelji slažu oko učinkovitosti ovih tehnika za izgradnju strategija trgovanja kako zbog ispravnosti temeljnih koncepata tako i zbog jednostavnosti provedbe. Među različitim kategorijama strategije koje dolaze iz sfere tehničke analize mogu se podijeliti na strategije koje prate trend (engl. *trend following strategy*) poput indeksa relativne snage, Bollingerovih ovojnica i Fibonaccijevih povlačenja te strategije vraćanja prosjeka (engl. *mean reverting strategy*)⁵² poput jednostavnih i eksponencijalnih pomičnih prosjeka. U ovome poglavlju osvrnut će se na glavne značajke osnovnih pokazatelja kriptovaluta, a primjeri će se bazirati na kriptovaluti kojom se najviše trguje, odnosno bitcoinu.

3.4.1. Indeks relativne snage (engl. *Relative Strength Index*)

RSI pokazatelj, koji je razvio tehnički analitičar Welles Wilder u svojoj knjizi *New Concepts in Technical Trading Systems* (1978.), pomaže trgovateljima da prepoznaju kada je cijena kriptovalute predaleko od njene „prave“ vrijednosti dopuštajući trgovatelju da iskoristi prednost prije nego što se tržište regulira. Koristeći RSI, trgovatelji mogu ostvariti sjajne ulazne točke za trgovanje, a s vremenom se ovaj pokazatelj pokazao kao neprocjenjiv alat za trgovanje nestabilnim kriptotržištima.

RSI koristi složenu formulu kako bi utvrdio je li imovina, u ovom slučaju, kriptovaluta prekupljena ili preprodana. Formula daje vrijednost koja se kreće između 0 i 100 i može se prikazati na grafikonu pomoću oscilatora uzorka tipa vala.

Prema Huangu i Kimu⁵³ vrijedi sljedeće:

$$U_i = \begin{cases} C_i - C_{i-1} & \text{ako } C_i > C_{i-1} \\ 0 & \text{ako } C_i < C_{i-1} \end{cases}$$

$$D_i = \begin{cases} C_{i-1} - C_i & \text{ako } C_{i-1} > C_i \\ 0 & \text{ako } C_{i-1} < C_i \end{cases}$$

Pri čemu U_i prikazuje uzlazni trend, D_i silazni, a C_i jest cijena zatvaranja u vremenu i .

⁵² Resta, M., Pagnottoni, P., De Giuli, M. E. (2020) Technical Analysis on the Bitcoin Market: Trading Opportunities or Investors' Pitfall?. *Multidisciplinary Digital Publishing Institute* [online], 8 (44), str. 4.

⁵³ Huang, K. i Kim, Y. S. (2006) *A Test of MACD Trading Strategy*. Burnaby: Simon Fraser University, str. 5

Najprvo određujemo silazno-uzlazne trendove. Navedeni iskaz hoće reći da ako je cijena zatvaranja u vremenu i veća od cijene zatvaranja u vremenu $i-1$, tada postoji uzlazni trend. S druge strane, ako je cijena zatvaranja u vremenu i manja od cijene zatvaranja u vremenu $i-1$, tada postoji silazni trend.

Potom se računaju eksponencijalni pomični prosjeci D_i i U_i .

$$\overline{U}_{t,p} = EMA(U_i)$$

$$\overline{D}_{t,p} = EMA(D_i)$$

Omjer ovih dvaju prosjeka daje *relativnu snagu* (RS).

$$RS_{t,p} = \frac{\overline{U}_{t,p}}{\overline{D}_{t,p}}$$

Konačno, možemo izračunati indikator RSI.

$$RSI_{t,p} = 100 - \frac{100}{1 + RS_{t,p}}$$

Pojednostavljena verzija formule glasi:

$$RSI = 100 - \frac{100}{(1 + RS)}$$

$$RS = \frac{AvgU \text{ (prosjeak svih uzlaznih kretanja u periodu X)}}{AvgD \text{ (prosjeak svih silaznih kretanja u periodu X)}}$$

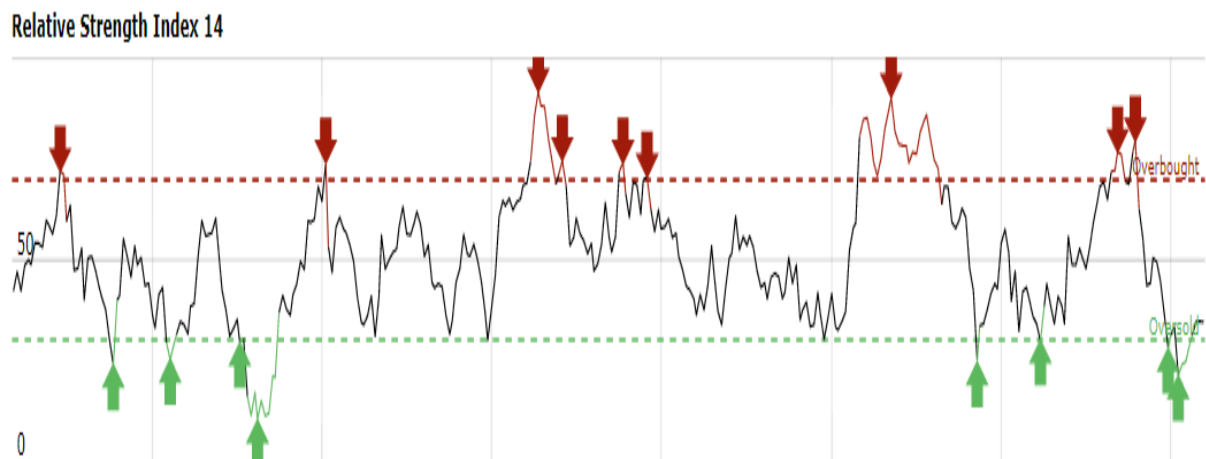
X - brojka se uzima proizvoljno, ali preporučena vrijednost iznosi 14.

Imovina se smatra preprodanom ili podcijenjenom kad RSI padne ispod 30 te u tom slučaju imamo kupovni signal. S druge strane, imovina se smatra prekupljenom ili precijenjenom ako RSI prijeđe 70 te dobivamo prodajni signal.

Korištenje indeksa relativne snage (RSI)

Jednom kada RSI dosegne 70, doći će do povlačenja, što se vidi ako se grafikon nalazi na području prekomjerne kupnje. Međutim, na sljedećem grafikonu može se uočiti da je tijekom padajućeg trenda RSI dosegnuo razinu od 50%, a ne 70%, što bi investitori mogli koristiti za pouzdanije signaliziranje međvjedih uvjeta. Mnogi će ulagači primijeniti vodoravnu liniju trenda koja se kreće između 30% i 70% za bolje prepoznavanje krajnosti.

Grafikon 4. Indeks relativne snage



Dostupno na: <https://www.cryptocompare.com/coins/btc/charts/USDT?ci0=BB20&t=LC&bc=RSI14>. [4.5.2021.]. Napomena: Crvene strelice označuju signal za prodaju, a zelene za kupnju.

3.4.2. Bollingerove ovojnice (engl. *Bollinger Bands*)

Bollingerove ovojnice alat su za tehničku analizu koji je razvio John Bollinger 1980-ih za trgovanje dionicama. One djeluju kao mjerač oscilatora, pokazujući ima li tržište visoku ili nisku nestabilnost ili čak postoje li uvjeti pretjeranog kupovanja i pretjerane prodaje. Glavna ideja koja stoji iza ovog pokazatelja jest pokazati kako su cijene raspoređene u prosječnoj vrijednosti. Bollingerove ovojnice sastoje se od gornjeg pojasa, pojasa pomičnog prosjeka i donjeg pojasa. Dva vanjska pojasa reagiraju na djelovanje tržišne cijene. Proširuju se (odmiču se od srednjeg pojasa) kada je volatilnost velika i skupljaju se (približavaju se srednjem pojasu) kada je volatilnost mala.

Standardne formule Bollingerovih ovojnica postavljaju središnju liniju kao 20-dnevni jednostavni pomični prosjek (SMA). Što se tiče gornjeg i donjeg opsega, oni se izračunavaju na temelju volatilnosti tržišta.⁵⁴

Središnja linija: 20-dnevni jednostavni pomični prosjek (SMA)

Gornji pojas: $SMA(TP, n) + m * \sigma[TP, n]$

Donji pojas: $SMA(TP, n) - m * \sigma[TP, n]$

Gdje je TP prosječna cijena najviše, najniže i cijene zatvaranja, n broj dana u periodu

⁵⁴ Hayes, A. (2020) *Bollinger Band® Definition* [online]. New York: Investopedia.

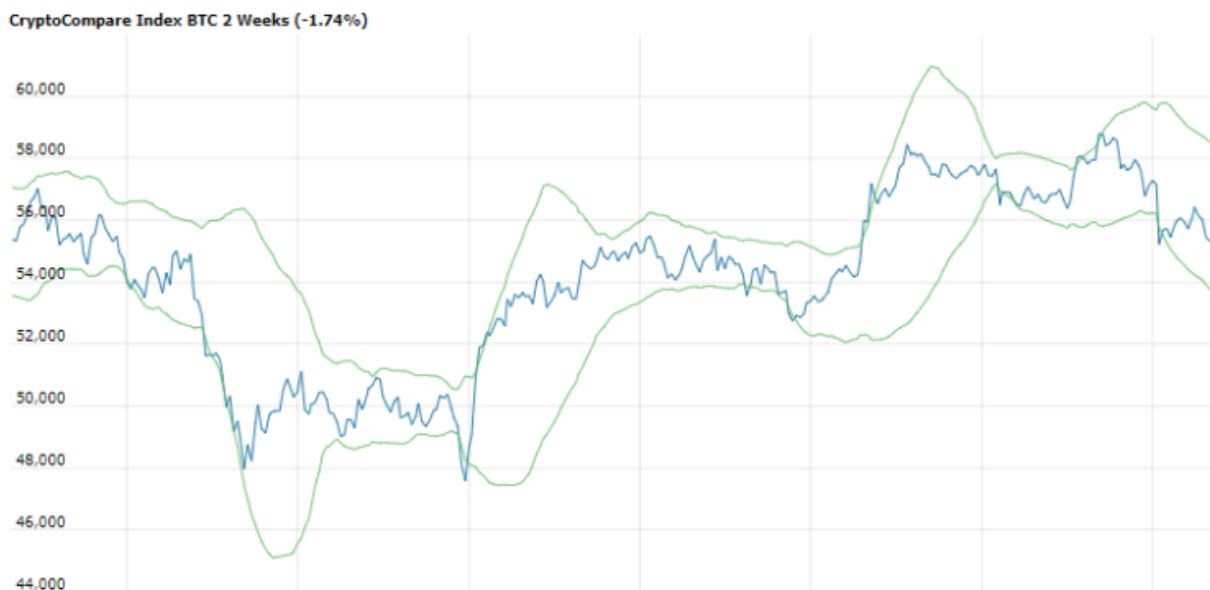
izgladivanja (obično 20), m broj standardnih devijacija (obično 2), $\sigma[TP,n]$ standardna devijacija tijekom n perioda TP .

Korištenje Bollingerovih ovojnica

Ako cijena imovine prijeđe pomični prosjek i premaši gornju Bollingerovu ovojnicu, možemo reći da je tržište u stanju prekomjerne kupnje (prekomjerno prošireno). S druge strane, ako cijena značajno padne i više puta premaši ili dodirne donji pojas, to je pokazatelj pretjerane prodaje na tržišta ili je cijena pronašla snažnu razinu potpore. Stoga su Bollingerove ovojnice prikladne za kratkoročno trgovanje jer mogu analizirati volatilitet tržišta i pokušati predvidjeti kretanja koja će vjerojatno doći.

Na sljedećem grafikonu indikator zaokružuje 20-dnevni SMA dionice gornjim i donjim pojasom, zajedno s dnevnim kretanjem cijene dionice. Budući da je standardna devijacija mjera nestabilnosti, kada tržišta postaju nestabilnija, pojasi se šire; tijekom manje volatilnih razdoblja, pojasi se skupljaju.

Grafikon 5. Bollingerove ovojnice



Dostupno na: <https://www.cryptocompare.com/coins/btc/charts/USDT?ci0=BB20&t=LC>. [4.5.2021.].

Napomena: Bollingerove ovojnice prikazane su zelenom linijom.

Stisak (engl. *squeeze*) i probijanje (engl. *breakout*)

Prema Hayesu (2020)⁵⁵ stisak je središnji koncept Bollingerovih ovojnica. Kad se pojasi približe, stežući pomični prosjek, to se naziva stiskom. Stisak signalizira razdoblje male volatiliteta i trgovci ga smatraju potencijalnim znakom buduće povećane volatiliteta i mogućih

⁵⁵ Hayes, A. (2020) *Bollinger Band® Definition* [online]. New York: Investopedia.

prilika za trgovanje. Suprotno tome, što se šire rasponi pomiču, to je veća vjerojatnost za smanjenje volatilnosti i veća je mogućnost izlaska iz trgovine. Međutim, ovi uvjeti nisu trgovački signali te ne daju naznake kada se promjena može dogoditi ili u kojem se smjeru cijena može kretati. Otprilike 90% cijena djeluje između dva pojasa. Pogreška većine ljudi jest vjerovanje da je cijena koja premaši ili premaši jedan od pojaseva signal za kupnju ili prodaju. Probijanja ne daju naslutiti smjer i opseg budućeg kretanja cijena.

Ograničenja Bollingerovih ovojnica

Iako su Bollingerove ovojnice korisni alati, postoji nekoliko ograničenja koja bi se trebala uzeti u obzir prije nego što ih se koristi. Jedno od tih ograničenja jest da su Bollingerove ovojnice nisu predviđajući indikatori. Opsezi će reagirati na promjene u kretanju cijena, bilo uzlazne ili padove, ali neće predviđati cijene. To je zato što se alat temelji na jednostavnom pomičnom prosjeku koji uzima prosječnu cijenu nekoliko cjenovnih pojaseva. Iako trgovatelji mogu koristiti opsege za procjenu trendova, ne mogu sami koristiti alat za predviđanje cijena. Još jedno ograničenje Bollingerovih ovojnica jest da standardne postavke neće raditi za sve trgovatelje. Učinkovitost Bollingerovih ovojnica razlikuje se od tržišta do tržišta, a trgovatelji će možda morati prilagoditi postavke čak i ako trguju istom imovinom tijekom određenog vremenskog razdoblja.

3.4.3. *Fibonaccijeve razine povlačenja (engl. Fibonacci Retracement Levels)*

Prema Mitchellu (2021)⁵⁶ u tehničkoj analizi Fibonaccijeve razine ukazuju na ključna područja na kojima se imovina može preokrenuti ili zaustaviti. Razine su prikazane vodoravnim crtama koje pokazuju gdje će se vjerojatno pojaviti potpora i otpor te se temelje na Fibonaccijevim brojevima. Svaka je razina povezana s postotkom, i to 23,6%, 38,2%, 61,8% i 78,6%. Iako službeno nije Fibonaccijev omjer, također se koristi 50%. Fibonaccijev niz izveden je iz zbroja prethodna dva broja koji se temelje na „zlatnom omjeru“. Niz započinje nulom i jedan. Zatim se dodaju prethodna dva broja da bi se dobio sljedeći niz brojeva:

- 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987 ... pri čemu se niz nastavlja neograničeno.

Sve Fibonaccijeve razine povlačenja izvedene su iz ovog brojevnog niza. Nakon započinjanja niza dijeljenjem jednog broja sa sljedećim brojem dobiva se otprilike 0,618 ili 61,8%.

⁵⁶ Mitchell, C. (2021) *Fibonacci Retracement Levels* [online]. New York: Investopedia.

Podijelivši broj s drugim brojem s njegove desne strane, rezultat je 0,382 ili 38,2%. Svi omjeri, osim 50% (budući da to nije službeni Fibonaccijev broj), temelje se na nekim matematičkim izračunima koji uključuju ovaj brojevni niz. Trgovanjem se može primijetiti da cijena redovito reagira na te razine te tako može ponuditi optimalne ulazne i izlazne točke. Međutim, prije upotrebe ovog pokazatelja za identificiranje potencijalne razine podrške ili otpora, potrebno je moći locirati najvišu (engl. *swing high*) i najnižu (engl. *swing low*) poziciju unutar određenog razdoblja.

Swing high jest točka na vrhuncu trenda u bilo kojem vremenskom okviru, dok je *swing low* najniža točka trenda. Kada se prepoznaju ove točke, možemo odabrati Fibonaccijev pokazatelj za praćenje u softveru za trgovanje i spojiti *swing low* na *swing high*. Na taj se način mogu generirati potencijalne razine podrške, poznate i kao povlačenja (engl. *retracements*). Svaka se razina potpore izvodi množenjem okomite udaljenosti „od najviše do najniže točke“ odnosima unutar Fibonaccijevog niza te zatim oduzimanjem od najviše točke.

Grafikon 6. Primjer Fibonnacijevih razina na tečaju bitcoin/dolar



Dostupno na: <https://www.tradingview.com/ideas/search/FIBONNACI%20RETRACEMENT/> [14.2.2021.].

Na prethodnom grafikonu možemo primijetiti kako je *swing low* za razdoblje od godine dana iznosio 3.000 BIT/USD, a *swing high* 20.000 BIT/USD. Kada se ovaj pokazatelj primijeni na grafikonu, korisnik odabire ove dvije točke. Jednom kada se te dvije točke odaberu, linije se crtaju u postocima prostora dvaju *swingova*. Kako se cijena tečaja mijenja, tako će razina od 23,6% biti na 15.998 BIT/USD ($20.000 \text{ BIT/USD} - (17.000 \text{ BIT/USD} \times 0,236) = 15.998 \text{ BIT/USD}$), razina od 38,2% bit će na 13.506 BIT/USD ($20.000 \text{ BIT/USD} - (17.000 \text{ BIT/USD} \times 0,382) = 13.506 \text{ BIT/USD}$), razina od 61,8% bit će na 9.494 BIT/USD ($20.000 \text{ BIT/USD} - (17.000 \text{ BIT/USD} \times 0,618) = 9.494 \text{ BIT/USD}$), razina od 78,6% bit će na 6.638 BIT/USD ($20.000 \text{ BIT/USD} - (17.000 \text{ BIT/USD} \times 0,786) = 6.638 \text{ BIT/USD}$), što je vidljivo i na

grafikonu.

3.4.4. Pomični prosjeci (engl. *Moving Averages*)

Pokazatelj pomičnih prosjeka koristi se za ujednačavanje cijena tijekom određenog razdoblja. MA je pokazatelj zaostajanja što znači da se temelji na prethodnom djelovanju cijena. Postoje dvije vrste pomičnih prosjeka: jednostavan pomični prosjek i eksponencijalni pomični prosjek. Izbor MA ovisi o stilu trgovanja. Dakle, kratkoročni trgovatelj odabrat će kraći MA, dok je duži MA pogodan za dugoročne trgovatelje. Razlog izračunavanja pomičnog prosjeka kriptovalute jest pomoć u izgladivanju podataka o cijeni stvaranjem stalno ažurirane prosječne cijene. Izračunavanjem pomičnog prosjeka ublažavaju se utjecaji slučajnih kratkoročnih kolebanja na cijenu tijekom određenog vremenskog okvira.

Jednostavni i eksponencijalni pomični prosjek

Najjednostavniji oblik pomičnog prosjeka ili **SMA**, izračunava se uzimajući aritmetičku sredinu zadanog skupa vrijednosti. Drugim riječima, skup brojeva - ili cijena u slučaju financijskih instrumenata - zbrajaju se i dijele s brojem cijena u skupu. Formula za izračunavanje jednostavnog pokretnog prosjeka jest sljedeća⁵⁷:

$$MA_t(k) = \frac{1}{k} \sum_{i=t-k}^t w_i \times P_i$$

Gdje je MA_t jednostavni pomični prosjek u razdoblju t , P_i cijena je zatvaranja za razdoblje i , k je pozitivan cijeli broj koji ne može prijeći prag $t/2$, a w_i težina cijene. Kada je w_i jednako 1, gornja formula vraća takozvani jednostavni pomični prosjek, dok u svim ostalim slučajevima vraća ponderirani pomični prosjek (engl. *weighted moving average* ili WMA). Signal za kupnju generira se kada cijena zatvaranja poraste iznad **SMA**, a signal za prodaju kada zatvaranje padne ispod **SMA**.

Eksponencijalni pomični prosjek⁵⁸ vrsta je pokretnog prosjeka koji daje veću težinu nedavnim cijenama. Da bi se izračunao EMA, prvo se računa jednostavni pokretni prosjek (SMA) tijekom određenog vremenskog razdoblja, a zatim množitelj za ponderiranje EMA (koji se naziva „faktor izravnavanja“), koji obično slijedi formulu: $[2 / (\text{odabrano vremensko razdoblje} + 1)]$. Dakle, za 20-dnevni pokretni prosjek množitelj bi bio $[2 / (20 + 1)] = 0,0952$.

⁵⁷ Resta, M., Pagnottoni, P., De Giuli, M. E. (2020) Technical Analysis on the Bitcoin Market: Trading Opportunities or Investors' Pitfall?. *Multidisciplinary Digital Publishing Institute* [online], 8 (44), str. 4.

⁵⁸ Fernando, J. (2021) *Moving Average* [online]. New York: Investopedia.

Potom se koristi faktor zaglađivanja u kombinaciji s prethodnom EMA da bismo dobili trenutnu vrijednost. EMA tako daje veći ponder nedavnim cijenama, dok SMA dodjeljuje jednak ponder svim vrijednostima.

$$EMA_t = [V_t \times \left(\frac{s}{1+d}\right)] + EMA_y \times [1 - \left(\frac{s}{1+d}\right)]$$

Gdje su EMA_t i EMA_y današnji i jučerašnji eksponencijalni pomični prosjeci, V_t današnja vrijednost, d broj dana, s faktor izravnjavanja.

Izračun EMA stavlja veći naglasak na nedavne podatke. Zbog toga se EMA smatra ponderiranim prosjekom. EMA brže reagira na promjenu cijena od SMA te ima veću vrijednost kada cijena raste od SMA (i pada brže od SMA kada cijena opada). Ova reakcija na promjene cijena glavni je razlog zašto neki trgovatelji radije koriste EMA nego SMA.

Korištenje pomičnih prosjeka

MA nagibi mogu pomoći trgovatelju da definira trend. Ako se ispostavi da MA ima nagib prema gore, to znači da je imovina u uzlaznom trendu ili da dobiva na cijeni, ali ako je MA nagnut prema dolje, to znači da je imovina koja se procjenjuje u padu ili gubi na cijeni. Grafikon 7. u nastavku prikazuje nagib koji se mijenja prema kraju, što sugerira da cijena ulazi u uzlazni trend, a grafikon 8. silazni trend. Važno je napomenuti da je MA pokazatelj zaostajanja. Stoga nagib pomičnog prosjeka može samo pomoći da se definira trend. Zbog toga jedan pomični prosjek nije dovoljno pouzdan da bi se mogao primijetiti prijelaz iz uzlaznog u silazni trend.

Grafikon 7. Jednostavni pomični prosjek



Izvor: Hayes, A. (2020) *Simple Moving Average (SMA)* [online]. New York: Investopedia. Dostupno na: <https://www.investopedia.com/terms/s/sma.asp>

Grafikon 8. Eksponencijalni pomični prosjek



Izvor: Hayes, A. (2020) *Exponential Moving Average (EMA)* [online]. New York: Investopedia. Dostupno na: <https://www.investopedia.com/terms/e/ema.asp>

Križanje (engl. *crossover*) s pomičnim prosjekom nudi još jedan popularan „stil“ trgovanja. Za trgovanje crossoverima na grafikonu se trebaju nalaziti dva ili više MA. Dopuštena su samo dva križanja kako bi se izbjeglo pretrpavanje grafikona i osiguralo da je jedan od pomičnih prosjeka (MA) duži od drugog. Dva popularna uzorka trgovanja koja koriste jednostavne pomične prosjeke uključuju križ smrti⁵⁹ i zlatni križ.⁶⁰

Zlatni križ (engl. *golden cross*) nastaje kada se kratkoročni SMA nalazi iznad dugoročnog SMA, što označuje bikov signal trgovanja te daljnje dobitke i rast cijena.

Križ smrti (engl. *death cross*) događa se kada 50-dnevni ili kratkoročni SMA prijeđe ispod 200-dnevnog ili dugoročnog SMA, što označuje medvjedi signal trgovanja te pad cijena i dobitaka.

⁵⁹ Chen, J. (2021) *Death cross definition* [online]. New York: Investopedia

⁶⁰ Chen, J. (2020) *Golden cross definition* [online]. New York: Investopedia.

4. RAZVOJ TRŽIŠTA KRIPTOVALUTA U HRVATSKOJ

4.1. Razvoj regulatornog okvira kriptovaluta u Hrvatskoj

Za javnost je, povrh svega, bitno znati je li upotreba kriptovaluta legalna, kako se pravno definira njihov status te na koji način ih tretirati kada je riječ o oporezivanju. Sve do danas relevantne financijske institucije objavile su tek nekoliko preporuka i naputaka o korištenju kriptovaluta u Republici Hrvatskoj. Iako u Republici Hrvatskoj ne postoji zakon o kriptovalutama, Porezna uprava Ministarstva financija u neku ruku uporište teži naći u postojećem *Zakonom o porezu na dohodak*. Prema navedenom mišljenju⁶¹ izdanom 14. srpnja 2017. godine navedeno je: *“Trgovanje kriptovalutama smatra se financijskom transakcijom (...) na dohodak ostvaren po osnovi trgovanja kriptovalutama plaća se porez na dohodak po osnovi kapitalnih dobitaka, budući se radi o dobitku po osnovi kupoprodaje te valute, što je ekvivalent instrumentima tržišta novca. Porez se plaća na razliku između nabavne i prodajne cijene umanjenoj za možebitne troškove trgovanja.”* Nadalje, porezni obveznik je *“obvezan porez na dohodak od kapitala po osnovi kapitalnih dobitaka, obračunati, obustaviti i uplatiti do posljednjeg dana mjeseca veljače tekuće godine za sve kapitalne dobitke ostvarene u prethodnoj godini, umanjene za ostvarene kapitalne gubitke.”* Porez se plaća po stopi od 12%, a potom se uvećava za prirez nadležne općine/grada. Iznimno se porez ne plaća ako imatelj kriptovalutu drži dulje od 2 godine. Treba naglasiti kako se ovdje radi o zamjeni kriptovaluta fiat valutama.

19. ožujka 2018. izdano je novo mišljenje⁶² koje je trebalo pojasniti različite okolnosti. Primjerice, *“Kod zamjene jedne kriptovalute za drugu ne utvrđuje se dohodak od kapitala budući da nema novčanog tijeka, odnosno nije došlo do zamjene kriptovalute za neku od valuta koje su priznate kao zakonsko sredstvo plaćanja”*, što želi reći da se zamjena kriptovalute u drugu kriptovalutu ne oporezuje. Što se tiče rudarenja, *„ako porezni obveznik rudarenje obavlja kontinuirano kroz duži period te mu je to osnovno zanimanje, tada je obvezan registrirati samostalnu djelatnost i dohodak utvrditi sukladno člancima 30. do 35. Zakona o porezu na dohodak.”* Veliki problem pod ovom točkom jest što nije definirano što je točno duži period. Međutim, dohodak koji rudar ostvari za svoj rad smatra se drugim dohotkom iz članka 39. *Zakona o porezu na dohodak*. Ako se kriptovaluta dalje koristi za trgovanje na burzama i na

⁶¹ Porezna uprava (2017) *Porezni tretman kapitalnih dobitaka po osnovi trgovanja kriptovalutama* [online]. Zagreb.

⁶² Porezna uprava (2018) *Porezni tretman kapitalnih dobitaka po osnovi trgovanja kriptovalutama* [online]. Zagreb.

kraju se zamijeni za npr. dolare, tada se plaća porez na temelju razlike između vrijednosti dobivene rudarenjem te prodane vrijednosti. Vrijednost rudarene kriptovalute utvrđuje se na temelju tečaja vodećih burzi na taj datum. Dana 18. prosinca 2017. Vijeće za financijsku stabilnost upozorilo je⁶³ da pojedinci koji ulažu u virtualne valute snose isključivu odgovornost za svoje gubitke i da trebaju biti svjesni mogućeg oporezivanja. Vijeće je izjavilo da hrvatski regulatorni organi nisu odgovorni za nadzor pojedinaca koji izdaju virtualne valute ili trguju njima. Vijeće je također primijetilo da su virtualne valute povezane sa značajnim rizicima, poput krađe digitalnog novčanika i zlouporabe transakcija, prijevara itd.

Od 1. siječnja 2020. poduzeća koja se bave trgovanjem virtualnih valuta i/ili pružaju skrbničku uslugu novčanika za čuvanje privatnih kriptografskih ključeva (npr. mjenjačnice kriptovaluta i poslovni subjekti koji se oslanjaju na kriptotransakcije) postali su obveznici *Zakona o sprječavanju pranja novca i financiranja terorizma*⁶⁴ koji čini dio implementacije 5. direktive Europske unije (EU) o sprječavanju korištenja financijskog sustava u svrhu pranja novca i financiranja terorizma, a za čiji je nadzor provođenja nadležna Hrvatska agencije za nadzor financijskih usluga (HANFA). Po ovom zakonu ciljane tvrtke morat će provoditi mjere dubinske analize svojih klijenata te sastaviti i koristiti liste indikatora za prepoznavanje transakcija, sredstava i osoba za koje postoji sumnja na pranje novca i financiranje terorizma. Usto će morati obavještavati Ured za sprječavanje pranja novca Ministarstva financija o sumnjivim transakcijama kao i sve ostalo što propisuje zakon.

Konačno, prema Hrvatskoj narodnoj banci: „*Virtualne valute nisu novac jer ne ispunjavaju osnovne funkcije novca, a na to posebno utječe velika kolebljivost njihove vrijednosti, kao i činjenica da se ponuda pojedine virtualne valute zasniva isključivo na tehnološkim rješenjima, a ne na potrebama gospodarstava ili monetarnog sustava. (...) nisu zakonsko sredstvo plaćanja (...), nisu strana valuta (deviza), (...) nemaju ni svojstva elektroničkog novca, a trgovanje i plaćanje virtualnim valutama ne može se smatrati platnom uslugom.*“⁶⁵ Nadalje, „*Jako korištenje virtualnih valuta nije ilegalno, u većini europskih država prevladava mišljenje da virtualne valute ne udovoljavaju pravnim kriterijima da bi mogle biti kvalificirane kao zakonsko sredstvo plaćanja, elektronički novac ili instrument plaćanja. (...) u postojećem regulatornom okviru institucije ne reguliraju niti nadziru kupnju, prodaju ili bilo koji drugi oblik ulaganja i korištenja virtualnih valuta.*“⁶⁶ Stoga, budući da kriptovalute nisu ilegalne, ali nisu ni pod

⁶³ Hrvatska narodna banka (2017) *9th Session of the Financial Stability Council* [online]. Zagreb.

⁶⁴ Narodne novine (2020) *Zakon o sprječavanju pranja novca i financiranja terorizma* [online]. Zagreb: Narodne novine d.d., 39 (19)

⁶⁵ Hrvatska narodna banka (2018) *Što su virtualne valute?* [online]. Zagreb.

⁶⁶ Hrvatska narodna banka (2018) *Što su virtualne valute?* [online]. Zagreb.

ingerencijom HNB-a, u HNB-u upozoravaju na moguće rizike za koje oni ne odgovaraju.

4.2. Primjeri hrvatskog poslovanja na tržištu kriptovaluta

Hrvatska je malo otvoreno gospodarstvo koje vrlo sporo prihvaća tehnološko-financijske inovacije. Unatoč tome, na tržištu su se istaknule pojedine tvrtke koje se bave kriptovalutama i koje nimalo ne zaostaju za svjetskim tržištem, a o čijem će poslovanju biti riječ dalje u tekstu.

Društvo Electrocoin d.o.o.⁶⁷ na tržištu se javlja kao posrednik u trgovanju kriptovalutama i procesiranjem kriptoupmeta, a osnovao ga je Nikola Škorić 2014. kako bi omogućio jednostavno, legalno i profesionalno trgovanje bitcoinom u Hrvatskoj, a kasnije mu se pridružio Marin Maržić kao suvlasnik i direktor tvrtke. Electrocoin je svoje poslovanje proširio čak i na čitavu Europsku uniju i na ostale značajne kriptovalute te zadržava mjesto kao najveći broker kriptovaluta u Hrvatskoj. Electrocoin je potpuno usklađen sa svim relevantnim regulativama u Republici Hrvatskoj te istovremeno radi na pribavljanju mišljenja i službenih stajališta o temama specifičnim za ovo novo područje, utvrđivanju zakonskih okvira te uspostavljanju veza s regulatornim tijelima u RH.

Njihova osnovna djelatnost podrazumijeva prodavanje i kupovanje kriptovaluta od fizičkih, pravnih i institucionalnih klijenata te omogućavanje trgovcima prihvaćanje upmeta u kriptovalutama u Hrvatskoj i ostatku Europske unije. Trgovanje se obavlja u kunama (HRK) i eurima (EUR) te u većini značajnijih kriptovaluta. Pored osnovnog poslovanja trgovanjem kriptovaluta Electrocoin razvija nekoliko projekata temeljenih na blockchain tehnologiji. Primjerice, društvo je uspostavilo vlastite web-stranice bitcoin-mjenjacnica.hr gdje nude usluge kupnje i prodaje kriptovaluta koristeći *LocalBitcoins* platforme ili izravnim kontaktom, *PayCek* uslugom omogućeno je lako pretvaranje više vrsta kriptovaluta u hrvatske kune tijekom procesa kupovine, bilo da je riječ o fizičkoj trgovini ili web-shopu. Nadalje, na web-portal leader.media 2.2.2021. objavljen je članak⁶⁸ prema kojemu već spomenuta platforma PayCek omogućuje plaćanje goriva i svih drugih proizvoda i usluga na svih 46 Tifon benzinskih postaja u Hrvatskoj. Prihvaćaju se valute bitcoin (BTC), ether (ETH), stellar (XLM), ripple (XRP) i EOS, a usluga je dostupna od 2. veljače 2021., čime je Tifon postao prvi u industriji nafte i plina koji je ušao na tržište kriptovaluta u Hrvatskoj. No Tifon nije bio jedini koji je Electrocoin prepoznao kao revolucionarnog partnera na području kriptovaluta. Naime, 23.2.2021. tportal.hr

⁶⁷ <https://electrocoin.hr/>

⁶⁸ Lider media – službena stranica (2021). *Na 46 benzinskih postaja u Hrvatskoj omogućeno je plaćanje kriptovalutama* [online]. Zagreb.

objavio je kako je najveći web-shop u Hrvatskoj Bazzar.hr uveo plaćanje kriptovalutama, a plaćanje se može ostvariti sa šest dostupnih kriptovaluta: bitcoin (BTC), ether (ETH), stellar (XLM), ripple (XRP), DAI i EOS preko platforme *PayCek*. Hrvatska pošta u suradnji s Electrocoinom omogućuje zamjenu kriptovaluta u HRK u 55 poštanskih ureda, a moguće je zamijeniti pet najčešće korištenih kriptovaluta (Bitcoin, Ethereum, Stellar, Ripple i EOS).

Tvrtka također nudi usluge razvoja, savjetovanja i edukacije vezano uz razne aspekte blockchain tehnologije i općenito povezane industrije te je suosnivač Udruge za blockchain i kriptovalute (UBIK) kojoj su ciljevi izgraditi i osnažiti hrvatsku blockchain zajednicu te se zajedničkim snagama suočiti s otvorenim regulatornim pitanjima. Uspješno poslovanje tvrtke pokazuje da postoji značajna i legitimna potražnja za zakonitom kupnjom i prodajom kriptovaluta, kako od fizičkih tako i od pravnih i institucionalnih klijenata koji žele biti izloženi tržištu kriptovaluta, koji žele plaćati kriptovalutama ili koji razvijaju blockchain rješenja koja zahtijevaju pristup kriptovalutama.

Upravno vijeće Hrvatske agencije za nadzor financijskih usluga (Hanfa) 7.5.2020. izdalo je rješenje⁶⁹ kojim je društvu **Griffon Asset Management d.o.o.**⁷⁰ za upravljanje alternativnim investicijskim fondovima iz Osijeka izdalo odobrenje za osnivanje i upravljanje otvorenim alternativnim investicijskim fondom s privatnom ponudom Passive Digital Asset. Fond se osniva kao otvoreni alternativni investicijski fond s privatnom ponudom za ulaganje u kriptoimovinu te je specijaliziran za ulaganje u bitcoin. Ulagatelji u Fond mogu biti osobe koje se u skladu sa zakonom koji uređuje tržište kapitala smatraju profesionalnim ulagateljima. Hanfa je odobrila i plan poslovanja fonda koji nije otvorenog tipa, već je njegova ponuda privatna – samo za ulagače koji podnesu ponudu za kupnju udjela od Hanfinog odobrenja za rad pa sve do prikupljanja minimalne vrijednosti imovine u iznosu od milijun kuna. U razdoblju početne ponude uplatu početnog iznosa ulaganja moguće je izvršiti u novcu ili unosom imovine, pri čemu se primaju isključivo uplate bitcoina. Iz Hanfe su naglasili da Fond, zbog svoje strukture ulaganja, ima izrazito visoki rizik za ulagatelje, stoga je namijenjen dugoročnim investitorima s visokom tolerancijom prema riziku te primjenjuje pasivnu investicijsku strategiju. Strategija Fonda je kupovina i držanje gotovo isključivo bitcoina te se u tome smislu Fond može smatrati pasivnim, a cijena udjela u fondu trebala bi što preciznije pratiti cijenu bitcoina izraženu u eurima. U slučaju značajnog pada vrijednosti bitcoina, Društvo neće

⁶⁹ Hrvatska agencija za nadzor financijskih usluga. (2020). *Upravno Vijeće Hanfe izdalo rješenje za osnivanje alternativnog investicijskog fonda za ulaganje u bitcoin* [online]. Zagreb.

⁷⁰ <https://www.griffon-am.hr/>

nastojati aktivno smanjivati izloženost Fonda bitcoinu s ciljem umanjavanja pada vrijednosti udjela Fonda. Fond će težiti potpunoj investiranosti imovine u bitcoin (do 100% neto vrijednosti imovine u bitcoin), u skladu s tržišnim uvjetima, pri čemu će se u drugim oblicima imovine nastojati držati samo onaj dio sredstava potreban za održavanje likvidnosti nužne za ispunjavanje obveza Fonda.

Digital Asset d.o.o. tvrtka je iz Splita osnovana 2013., a čiji je vlasnik i direktor poduzetnik Tomislav Vajić. Tvrtka ističe kako su posvećeni uvođenju viših standarda u bitcoin zajednicu te da su prvi koji su uveli napredno upravljanje narudžbama u nestabilnoj bitcoin industriji. Osim Digital Assetom Vajić se može pohvaliti i inovacijom BitKonan, odnosno burzom i mjenjačnicom kriptovaluta, gdje su usluge otvorene prema inozemnom i tuzemnom tržištu, a službena je valuta američki dolar (USD) te se sve ostale konvertiraju u istu. Nakon prve burze kriptovaluta 2018. predstavio je i prvu fizičku mjenjačnicu kriptovaluta u Hrvatskoj *Bitcoin Store* s poslovnica u Splitu i Zagrebu, koje su dotada bile viđene samo u Americi, Francuskoj ili pak Japanu.

Digital Assets Power Play (DPP) d.o.o.⁷¹ pružatelj je najnaprednije algoritamske platforme za kriptotrgovanje i usluga na tržištu. Kako kažu, cilj im je osnažiti kriptotrgovce i omogućiti svima da trguju poput profesionalaca koristeći snagu algoritamskog trgovanja. DPP platforma intuitivni je kreator algoritamske strategije koji povezuje trgovce s više od 14.000 tržišta na više od 100 burzi uz pristup sveobuhvatnim značajkama pregleda tržišta, protoku podataka, povijesnim podacima, prosljeđivanju, upravljanju portfeljem i još mnogo toga. Usluge strujanja podataka na razini poduzeća i povijesne podatkovne usluge također su dostupne s DPP DataStreams i DPP Historical. DA Power Play bit će dostupan na uređajima iOS i Android, ali i kao desktop aplikacija. Omogućit će korisnicima da izgrade, simuliraju i upravljaju osobnim algoritamskim strategijama trgovanja. Platforma pruža korisnicima povijesne, ali i trenutne podatke s 20-ak svjetskih burzi, kao i tehničke pokazatelje, integrirajući ostale podatke poput feedova vijesti, društvene feedove i kretanje tržišta, omogućujući algoritmima da upravljaju digitalnim sredstvima te rizicima.

Ideja na kvadrat d.o.o.⁷² mala je tvrtka koja obavlja specijalističke projekte iz područja IT-a. Tvrtka je „solopreneur“ projekt dr. sc. Ivana Vorasa. Na službenoj stranici navode sljedeće

⁷¹ <https://www.dapowerplay.com/>

⁷² <https://www.idejanakvadrat.hr/>

područja u kojima pružaju usluge: bitcoin, kriptovalute i kriptografija, informacijska sigurnost, Internet of Things i elektronika, uspostavljanje i optimizacije baza podataka, SQL i NoSQL, optimizacija nabave i korištenja IT resursa. Tvrtka se također bavi dizajnom i izradom blockchaina, analizom blockchaina, izgradnjom payment gatewaya, stvaranjem altcoina i analizom i prilagođavanjem korištenih algoritama.

FIMA Plus d.o.o.⁷³ vlasnika Milana Horvata iz Varaždina društvo je specijalizirano za pružanje usluga na kriptotržištu. Dio je sustava FIMA, koja ima više od 25 godina iskustva na domaćim i stranim tradicionalnim financijskim tržištima. Tvrtka vodi servis Fima Pay te u suradnji s tvrtkom Neoinfo nudi uslugu plaćanja kriptovalutama na Adeo POS blagajnama. Nudi usluge čuvanja kriptovaluta te konverzije

Od ostalih tvrtki aktivnih na ovom području treba spomenuti IN KAPITAL d.o.o. kao prvu tvrtku u Hrvatskoj čije su mjenjačnice počele pružati usluge kupovine i prodaje kriptovaluta, blokIdea d.o.o., TIKOMAR d.o.o. te Node Factory d.o.o. koji su također svojim inovacijama doprinijeli izgradnji kriptotržišta.

4.3. Primjeri izdavanja kriptokovanica u Republici Hrvatskoj

ICO (engl. *Initial Coin Offering*) predstavlja ekvivalent industrije kriptovaluta početnoj javnoj ponudi (engl. *Initial Public Offering* ili IPO). Tvrtka (u pravilu *startup*) koja želi prikupiti novac za stvaranje nove valute, aplikacije ili usluge pokreće ICO kao način prikupljanja sredstava. Zainteresirani ulagači mogu kupiti ponudu i dobiti novi token kriptovalute koji je izdala tvrtka. Ovaj token može imati korisnost u korištenju proizvoda ili usluge koju tvrtka nudi ili može samo predstavljati udio u tvrtki ili projektu.

Već spomenuti **Digital Assets Power Play**, financijsko-tehnološki startup za automatizaciju trgovanja digitalnim valutama, bio je prva tvrtka koja je zaključila prvi uspješni ICO u Hrvatskoj. U samo tjedan dana *startup* je prešao minimalnu kapitalizaciju od 2,1 milijuna američkih dolara i prikupio ukupno 2,6 milijuna dolara (ili 8,479 jedinica kriptovalute pod nazivom ether, u sklopu mrežnog protokola ethereum). 19. rujna 2017. u 17 sati započelo je prikupljanjem sredstava na prvom hrvatskom ICO-u te je nakon dva dana pretprodaje slijedila petodnevna javna faza prodaje. Minimalni ciljani iznos crowdfunding kampanje iznosio je 2,1

⁷³ <https://fimaplus.com/>

milijuna američkih dolara (8,236 u kriptovaluti ether), dok su najviša očekivanja bila postavljena na 5,1 milijun dolara ili 20,000 ethera za 25 posto tokena. S web-portala zimo.dnevnik.hr prenose: „DPP tokeni (100,000,000 izdanih jedinica) novostvorena su kriptovaluta koja će se koristiti za stvaranje distribuirane ekonomije između zainteresiranih stranaka na globalnoj platformi, uključujući – ali ne ograničavajući se na – hedge fondove, upravitelje imovine, trgovce, razvojne programere i investitore. DPP tokeni koristit će se kao sredstvo plaćanja za obavljene usluge na platformi i prijenos vrijednosti, stvarajući peer-to-peer ekonomiju za korisnike baze platforme omogućenu pametnim ugovorima i blockchain tehnologijom. DPP tokeni bit će izlistani na nekoliko kriptoburzi širom svijeta čineći DPP tokene dostupne svima.“⁷⁴

Startup **Tolar.io** ili skraćeno **Tolar** predstavlja globalnu platformu za nove ICO-projekte razvivši tehnološko rješenje, HashNET, koje je zadržalo sve dobre strane blockchain tehnologije, a donijelo rješenja za velike nedostatke blockchaine poput brzine transakcija, skalabilnosti te potrošnje energije. Svoj vlastiti ICO⁷⁵ završio je 20. rujna 2018. Ukupni iznos prikupljen tijekom privatne prodaje, pretprodaje i ICO-a iznosi 28.807,01 ETH, što po tadašnjoj cijeni te kriptovalute od 406,72 dolara znači da je od investitora prikupio vrijednost veću od 11 milijuna dolara. 20.000 ETH bila je donja granica ili *soft cap* koji su si u Tolaru postavili za vlastiti ICO, a gornja granica ili *hard cap* 45.000. Osim toga, prema web-portalu poslovni.hr⁷⁶ Tolar se ističe kao prvi hrvatski startup koji je, da bi prikupio kapital za rast i razvoj, napravio globalni investicijski roadshow (nešto što su do sada radile isključivo najveće hrvatske kompanije i ministri financija). Počeo je na dva mjesta u isto vrijeme Seulu i Kuala Lumpuru, a zatim u Singapuru, Bangkoku, Hanoiu, Bahrainu, Ho Chi Minhu, ponovo Seulu te konačno u Tokiju, gdje je na predstavljanju japanskim kriptoinvestitorima na World Blockchain Roadshowu, Tolar dobio nagradu "Future of Blockchain". Turneju su nastavili na Mauricijusu, zatim je uslijedio Toronto, Perth, još dva puta Singapur pa Šangaj, da bi na koncu sve finalizirali u Londonu, Dubaiju i Moskvi.

Ostali *startupi* koji su proveli ICO jesu CookUp, platforma za naručivanje hrane i razmjenu znanja koja se odnosi na kuhanje te koja povezuje sve koji kuhaju s ljudima koji trebaju kvalitetne domaće obroke i Cryptotask, vrijedan milijun dolara, *startup* za prvu burzu rada na

⁷⁴ Čizmić, M. (2017) *Uspješno završen prvi ICO u Hrvatskoj* [online]. Zagreb: Zimo Dnevnik.

⁷⁵ <https://tolar.io/tokensale#token-metrics>

⁷⁶ Ivezić, B. (2018) *Najveći hrvatski ICO skupio 8,1 milijun dolara i ide po još* [online]. Zagreb: Poslovni dnevnik.

svijetu na kojoj će poslodavci i radnici moći biti i ljudi i strojevi.

4.4. Mogućnost uvođenja digitalne valute središnjih banaka u Hrvatskoj

Posljednjih godina bankama, kao financijskim institucijama, ključan izazov predstavljaju rastuća digitalizacija, sve manja upotreba gotovine uz snažan razvoj novih bezgotovinskih načina plaćanja te konkurencija FinTech tvrtki. Tako su banke postale svjesne da moraju reagirati na nove trendove ako žele zadržati dominantnu poziciju u financijskom sektoru. Nadalje, stabilne kriptovalute (engl. *stable coins*) kreirane su kako bi se prevladale nestabilnosti kriptovaluta prve generacije. Razvitkom ove hibridne kriptovalutne arhitekture, koja sadržava i obilježja kriptovaluta i obilježja e-novca, te postupnim smanjenjem fluktuacije vrijednosti u odnosu na referentne valute (poput američkog dolara ili eura) ili košaru valuta (koja se sastoji od nekoliko glavnih globalnih valuta) otvorilo se pitanje utjecaja na monetarnu politiku i financijsku stabilnost, bankovni sustav, kontrolu pranja novca, zaštitu potrošača i sl. Ovo pitanje iznjedrilo je porast inicijative koja se odnosi na uspostavu digitalnih valuta središnjih banaka (engl. *Central Bank Digital Currency*⁷⁷), a koje predstavljaju obvezu središnjih banaka u digitalnom obliku kojom se mogu koristiti građani i poduzeća za svoja plaćanja.

Valja istaknuti kako jedna vrsta centralnobankarskoga digitalnog novca zapravo već postoji, a to je onaj novac na otvorenim digitalnim računima poslovnih banaka kod središnje banke. Oni se koriste pri provođenju monetarne politike te osiguravanju učinkovitoga i stabilnoga platnog prometa. Građani, s druge strane, imaju pristup novcu središnje banke samo u fizičkom obliku, a ne i u digitalnom, a radi se o novčanicama i kovanicama kojima građanstvo svakodnevno raspolaže. Za razliku od prethodne dvije vrste novca, novac na računima i depozitima svih sektora gospodarstva kod poslovnih banaka jest obveza poslovne, a ne središnje banke. Stoga je glavno obilježje CBDC-a to što bi on bio digitalni novac središnje banke za sve korisnike financijskog sustava, a ne samo za poslovne banke, što se prije svega odnosi na stanovništvo te bi bio obveza središnje banke, kao i gotov novac. CBDC bi tako trebao biti potpuno jednak digitalnom novcu kojim se danas plaća/štedi putem nekog od postojećih digitalnih kanala – internet/mobilno bankarstvo, kartice itd. U osnovi je riječ o digitalnom ekvivalentu gotovom novcu, a njihovom uspostavom ostvario bi se pravi pomak u monetarnoj i platnoj arhitekturi. U nastavku rada će se analizirati potencijalno uvođenje verzije digitalne kune, odnosno digitalnog eura na čijem stvaranju Europska unija u trenutku pisanja ovoga rada aktivno radi.

⁷⁷ Dalje u tekstu koristit će se kratica CBDC.

4.4.1. Uvođenje digitalne kune

Digitalna bi kuna, prema dosadašnjim definicijama CBDC-a, trebala biti isto što i papirnata kuna, ali u digitalnom obliku. To bi značilo da bi HNB u njezinom kreiranju imao istu ulogu kao i sada te bi osiguravao njenu stabilnost i izdavao bi ju paralelno s papirnatom. Osim toga, digitalna kuna bila bi jednostavnija u korištenju, kao što su to virtualne kriptovalute poput bitcoina. Glavne prednosti mogle bi se vidjeti u našim glavnim gospodarskim granama, turizmu i trgovini. Naime, digitalna kuna mogla bi učiniti transakcije njome jeftinije od onih s gotovinom. Tako bi, primjerice, u turizmu, industriji koja značajno ovisi o gotovini, HNB i Ministarstvo financija mogli dati poduzetnicima priliku da ostvare značajne uštede zbog visokih troškova manipulacije gotovinom. Hrvatsko tržište pokazalo se kao dosta poželjno mjesto u Europi za testiranje financijskih inovacija. S obzirom na to da prima značajan broj turista, tako generira zanimljiv volumen, a opet po broju stanovnika tržište nije veliko te bi se svaki tržišni eksperiment lako mogao kontrolirati. Treba istaknuti kako digitalna kuna ne bi bila isto što i recimo bitcoin jer bi njome i dalje u cijelosti upravljao HNB, a ne isključivo zakon ponude i potražnje kao u slučaju kriptovaluta. Nadalje, budući da bi digitalna kuna ionako u nekom trenutku bila zamijenjena budućim digitalnim eurom, ovaj bi projekt isto tako mogao postati predložak za digitalni euro, a postao bi i predložak za druge države diljem svijeta koje žele uvesti vlastitu nacionalnu kriptovalutu, posebice države Europske unije koje čine tzv. članice s odstupanjem⁷⁸. Prema Ljubaju i Martinčeviću⁷⁹ zbog strateške opredijeljenosti k uvođenju eura, te s obzirom na to da je ESB nedavno započeo javnu raspravu o mogućem budućem izdavanju tzv. digitalnog eura, više je izgledno kako bismo u Hrvatskoj prije mogli imati digitalni euro nego digitalnu kunu. Isto tako, uzevši u obzir postojeće značajke našega monetarnog sustava i velika uloga koju i dalje ima gotov novac, digitalna kuna ni za HNB ni za hrvatske građane zapravo još nema značajnu ekonomsku ni stratešku opravdanost.

Međutim, uvođenje digitalne kune zasigurno bi za sobom povuklo i znante prednosti. Primjerice, znanje koje bi se time akumuliralo u financijskom i IT sektoru u Hrvatskoj, moglo bi postati važnim izvoznim proizvodom, a pružilo bi i perspektivu snažnim IT poslovanjima u Hrvatskoj koja razvijaju proizvode koji se kasnije prenose u druge države u sklopu njihovih grupacija. To bi također bila i prilika za otvaranje novih radnih mjesta u financijskom sektoru, kojem slijedi val otpuštanja u bankama zbog digitalne transformacije. Sve su to razlozi u korist uvođenja

⁷⁸ Bugarska, Češka, Hrvatska, Mađarska, Poljska, Rumunjska i Švedska čine članice s odstupanjem, odnosno države koje još uvijek nisu prihvatile euro kao službenu valutu.

⁷⁹ Ljubaj, I. i L. Martinčević. (2020). *Centralnbankarski digitalni novac – nova moda ili stvarna potreba?* Zagreb: Hrvatska narodna banka.

digitalne kune te zašto bi bilo dobro da Ministarstvo financija, HNB i HANFA pokrenu taj projekt. Otvoreni pitanja i izazovi bez sumnje je jako puno te još uvijek nije poznato bi li koristi od uvođenja CBDC-a premašile troškove i rizike. Razvoj platnih sustava i digitalnih načina provođenja transakcija svakako ide u korist ideji uvođenja CBDC-a, no kako je pokretanje CBDC-a složen koncept te se uvelike temelji na stvarnim potrebama gospodarstava i mogućim unapređenjima zadaća središnjih banaka, moglo bi proći još dosta vremena prije nego bilo kakav oblik nacionalne kriptovalute zaživi u Hrvatskoj.

4.4.2. Uvođenje digitalnog eura

Prema Vladi Republike Hrvatske ciljni datum uvođenja eura i dalje ostaje 1. siječnja 2023⁸⁰. Stručnjaci iz ECB-a i nacionalnih središnjih banaka europodručja postavili su niz osnovnih zahtjeva za digitalni euro, kao što su laka dostupnost, sigurnost, učinkovitost, privatnost i poštivanje zakona te bi početak projekta digitalnog eura, ako sve bude po planu, svjetlo dana trebao ugledati već sredinom 2021. godine⁸¹. S obzirom na to i hrvatsko će stanovništvo imati pristup ovoj kriptovaluti. Bez obzira na tehnologiju koja se koristi za digitalni euro, što bi također mogao biti tipični blockchain i kriptografija, njezina će priroda biti sasvim drugačija jer i dalje će biti u odgovornosti ECB-a, što znači da bi vrijednost eura u obliku gotovine bila jednaka vrijednosti digitalnog eura. Sveukupni cilj jest pružiti potrošačima više prostora za donošenje odluka i više mogućnosti u odabiru financijskih usluga i modernih platnih sustava. Na području plaćanja i financijskih usluga posljednje desetljeće u Europskoj uniji bilježi sve veći broj pružatelja usluga i inovativnih tehnologija i proizvoda. Čak i prije Covid-19 pandemije zabilježen je dubok pomak u preferencijama plaćanja, pri čemu je uporaba gotovine u maloprodaji opadala, a pandemija je ovaj trend samo još dodatno ubrzala. Digitalni euro imao bi za cilj podržati digitalizaciju istovremeno nastavljajući pružati ljudima mogućnost izbora načina plaćanja i osiguravajući da njihova plaćanja ostanu konkurentna i sigurna. Bio bi dizajniran da bude siguran, bez troškova, lako dostupan i jednostavan za upotrebu podržavajući financijsku uključenost. Zaštita privatnosti bila bi ključni prioritet pomažući pritom održavanju povjerenja u plaćanja.

Nadalje, digitalni euro bio bi dostupan kućanstvima, tvrtkama, trgovcima i financijskim posrednicima za plaćanja širom eurozone, čime bi pomogao u ujedinjenju europskog tržišta.

⁸⁰ Vlada Republike Hrvatske. (2021). *Ciljni datum uvođenja eura i dalje ostaje 1. siječnja 2023*. [online].

⁸¹ Fantesini, A. (2021). *Digital Euro, advantages and risks of the ECB's new virtual currency* [online]. Rim: Institute for Competitiveness.

Povećao bi izbor potrošača, smanjio transakcijske troškove i podržao digitalizaciju gospodarstva istovremeno osiguravajući da novac središnje banke ostane u srži financijskog sustava podupirući stabilnost. Digitalni euro također bi mogao djelovati kao katalizator na međunarodnoj razini. Osiguravanjem interoperabilnosti sa stranim digitalnim valutama te uključujući ostale digitalne valute središnje banke (CBDC), mogla bi se stvoriti prijeko potrebna dobit u učinkovitosti prekograničnih plaćanja smanjujući njihove troškove. Digitalni euro kombinirao bi učinkovitost digitalnog platnog instrumenta sa sigurnošću novca središnje banke, a ljudi koji koriste digitalni euro imali bi istu razinu povjerenja kao i kod gotovine jer ih oboje podržava središnja banka, što je nešto što kryptoimovina poput *stable coins*a ne može pružiti. Međutim, digitalni euro i dalje bi bio euro poput novčanica, ali u digitalnom obliku. Bio bi to elektronički oblik novca koji izdaje Eurosustav (ECB i nacionalne središnje banke) i bio bi dostupan svim građanima i tvrtkama te ne bi zamijenio novac, već bi ga nadopunio.

S druge strane, ako nije pravilno dizajniran, digitalni bi euro mogao utjecati na financijsko posredovanje i raspodjelu kapitala, na financijsku stabilnost u doba krize te na funkcioniranje međunarodnog financijskog sustava. Primjerice, mogao bi privući platnu aktivnost banaka i smanjiti njihov prihod povezan s plaćanjem. Također bi mogao privući depozite, pogotovo ako bi se nudio bez ograničenja i pod atraktivnim uvjetima, tako da bi javnost premještala velike iznose poslovnih banaka u središnje banke. To zabrinjava jer bi moglo dovesti do manje stabilnog i skupljeg financiranja, niže profitabilnosti banaka i, u konačnici, manjeg kreditiranja ograničavajući financiranje realne ekonomije. Ipak, Fabio Panetta, član Izvršnog odbora ECB-a, u svom govoru izjavio je kako ECB nema namjeru zamijeniti poslovne banke izravnim kontaktom s potencijalno stotinama milijuna korisnika digitalnog eura, već bi osigurali siguran novac, dok bi financijski posrednici i dalje nudili dodatne usluge korisnicima.⁸²

Nadalje, digitalni euro mogao bi poboljšati raspodjelu kapitala olakšavajući pristup plaćanjima i smanjujući transakcijske troškove pomažući tako ostvarivanju poslovnih prilika. Također bi mogao pojačati konkurenciju na tržištima financiranja banaka. Pri tome bi se smanjila tržišna snaga komercijalnih banaka i poboljšali bi se ugovorni uvjete za kupce. Osim toga, rizici financijskog posredovanja pri izdavanju digitalnog eura potencijalno su izraženiji u kriznim vremenima s obzirom na to da bi digitalni euro dao pristup sigurnoj likvidnoj imovini koja bi se, za razliku od gotovine, mogla držati u velikim količinama i bez ikakvih troškova. Dapače, ako nije pravilno dizajniran, u kriznim vremenima digitalni euro mogao bi ubrzati digitalne *bank runove* od poslovnih banaka prema središnjoj banci, što bi pak dovelo do toga da štediše

⁸² Panetta, F. (2021). *Evolution or revolution? The impact of a digital euro on the financial system* [online]. Frankfurt na Majni: Europska centralna banka.

smanjuju svoje bankovne depozite i pojačavaju volatilnost i u normalno vrijeme.

Povrh toga, digitalni euro mogao bi utjecati na financijski sustav i na prekograničnoj razini. Digitalni euro dostupan nerezidentima mogao bi jedinstvenu valutu učiniti privlačnijim kao sigurno sredstvo plaćanja za prekogranične maloprodajne transakcije. Na primjer, mogao bi pomoći u rješavanju neučinkovitosti u prekograničnoj infrastrukturi plaćanja i olakšati prijenos doznaka. No, ako digitalni euro ne bi bio dizajniran na način koji bi ga spriječio da se koristi kao oblik ulaganja, te bi koristi došle uz rizik pojačavanja međunarodnih šokova. Činjenica da bi digitalni euro bio vrlo likvidan može dovesti do toga da ga inozemni ulagači koriste nesrazmjerno, što bi dalje dovelo rezultiralo većim oscilacijama tečaja i imalo bi snažniji učinak na strane financijske uvjete.

Prema Panetti⁸³, da bi se postigle prednosti digitalnog eura, trebao bi biti pažljivo osmišljen te biti učinkovito sredstvo plaćanja na domaćem i međunarodnom nivou. Neželjene posljedice moglo bi se izbjeći dizajniranjem sustava koji omogućava digitalni euro za domaća i međunarodna plaćanja, ali koji ograničava njegovu upotrebu u investicijske svrhe. Jedna od mogućnosti bila bi ograničenje posjedovanja digitalnih eura. Jedan od načina da se to učini, iako bi se digitalni euro mogao koristiti za velike transakcije, bio bi zahtijevanje preusmjeravanja dolaznih sredstava koja premašuju ograničenje korisnika na bankovni račun, što bi spriječilo velike i/ili nestabilne priljeve bankovnih depozita u središnju banku. Druga opcija bila bi postavljanje kazni, kao što su negativne kamatne stope, na digitalne posjede iznad određenog praga, za koje je Panetta sugerirao da bi mogle iznositi 3000 eura. Do tog praga, iznosi u digitalnom euru nikada ne bi bili podložni negativnim kamatnim stopama i stoga se nikada ne bi tretirali manje povoljno od gotovine. Iznad tog praga, naknada bi se postavila tako da su veća držanja digitalnog eura profitabilna samo za veća plaćanja, a ne kao stalni oblik ulaganja.

Konačno, trajna digitalizacija novca i plaćanja svakako dovodi u pitanje uspostavljenu strukturu financijskog sustava. Digitalni euro predstavlja prirodni razvoj kao odgovor na ovu transformaciju jer ne samo da podupire učinkovitost i inovacije već i čuva ulogu središnjih banaka u pružanju sigurnih načina plaćanja. Kroz povijest se ta sigurnost pokazala presudnom u održavanju povjerenja javnosti u novac i u konačnici u državu. Stoga bi ključni cilj digitalnog eura trebao biti očuvanje fine ravnoteže između državnog i privatnog novca kako bi se osiguralo da plaćanja ostanu stabilna i učinkovita.

⁸³ Panetta, F. (2021). *Evolution or revolution? The impact of a digital euro on the financial system* [online]. Frankfurt na Majni: Europska centralna banka.

5. ZAKLJUČAK

Bitcoin i druge kriptovalute predstavljaju ideal koji bi mogao destabilizirati trenutnu infrastrukturu banaka i drugih financijskih institucija. Blockchain nudi distribuirane, sigurne i pouzdane arhitekture s kojima se konvencionalne tehnologije ne mogu natjecati. Činjenica da su ovakvi sustavi sigurniji od tradicionalnih leži u istraživačkom području dubokog učenja, kriptografiji, koje koristi mnoge napredne matematičke tehnike kojima se kontrolira ponuda i provode se različite sigurnosne mjere kako bi se spriječile prevare. Iako bankarska industrija predviđa poremećaj ulaganjem u ovu novu tehnologiju, mnogi će njezini poslovni modeli i tokovi prihoda biti pogođeni, posebno povećanom konkurencijom tehnološke industrije.

Jedna od većih prednosti kriptovaluta jest njihova decentralizarnost, što znači da nisu centralne banke one institucije koje izdaju kriptovalute, već pojedinci koji se nazivaju rudarima, a koji služeći se naprednim algoritmima i tehnologijama utječu na volumen kriptovaluta u optjecaju i svojom vještom verifikacijom doprinose integritetu kriptozajednice. Ono što može izazvati brigu oko kriptovaluta jest njihova iznimna volatilitnost. Međutim, analitičari su s vremenom razvili brojne matematičke modele i kriptopokazatelje koji u kombinaciji s tehničkom analizom mogu pomoći u predviđanju kretanja cijena kriptovaluta s većom točnošću. Prilike, ali i rizici, veliki su za financijski sektor.

S jedne strane, prednosti leže u anonimnosti i zaštiti privatnosti, jeftinijim elektroničkim transakcijama te već spomenutoj decentralizaciji. S druge strane, postoje zabrinutosti da će takav sustav labave regulacije olakšati aktivnosti crnog tržišta te izbjegavanje poreza. U svakom slučaju, može se zaključiti da su kriptovalute unotoč poteškoćama problemima s kojima se svjetsko tržište kriptovaluta susrelo i s kojima će se susresti u budućnosti pokazale da imaju svoje mjesto u financijskoj zajednici. Prilog u tome ide činjenica da je čak i Republika Hrvatska, kao malo otvoreno, ali još uvijek tradicionalno gospodarstvo dosta oprezeno prema financijskim inovacijama, otvorila svoja vrata kriptovalutama, što se vidi po brojnim tvrtkama čije inovacije ne zaostaju za onima svjetskima. Iako je društvo možda još uvijek u ranoj fazi korištenja kriptovaluta u svakodnevnim transakcijama, interes za kriptovalute i dalje raste, a njihovi se potencijalni programi, infrastrukture i broj tvrtki koje ih prihvaćaju svakodnevno se povećavaju. Na pragu smo nove financijske budućnosti, one u kojoj će potrošači širom svijeta imati pristup neometanoj razmjeni digitalne imovine i prednostima koje kriptovalute pružaju nad fiat valutama i drugim tradicionalnim načinima plaćanja.

LITERATURA

1. Akinci, E. i Li, J. (2015) *Bitcoin and Stock Market Indexes Causality* [online]. Jönköping: Jönköping University. Dostupno na: <https://www.diva-portal.org/smash/get/diva2:1214359/FULLTEXT01.pdf> [31.1.2021.]
2. Auer, R. i Claessens, S. (2018) *Réglementation des cryptomonnaies : évaluation des réactions du marché* [online]. Basel: Bank for International Settlements. Dostupno na : https://www.bis.org/publ/qtrpdf/r_qt1809f_fr.pdf [1.2.2021.]
3. Chen, J. (2021) *Death cross definition* [online]. New York: Investopedia. Dostupno na: <https://www.investopedia.com/terms/d/deathcross.asp> [21.2.2021.]
4. Chen, J. (2020) *Golden cross definition* [online]. New York: Investopedia. Dostupno na: <https://www.investopedia.com/terms/g/goldencross.asp> [21.2.2021.]
5. Connors, L. i Alvarez, C. (2013) *Bollinger Bands® Trading Strategies That Work*. [online]. Jersey City: Connors Research LLC. Dostupno na: <https://www.pdfdrive.com/bollinger-bands-trading-strategies-that-work-e13649215.html> [25.2.2021.]
6. Čizmić, M. (2017) *Uspješno završen prvi ICO u Hrvatskoj* [online]. Zagreb: Zimo Dnevnik. Dostupno na: <https://zimo.dnevnik.hr/clanak/da-power-play-uspjesno-završen-prvi-ico-u-hrvatskoj---490686.html> [31.3.2021.]
7. Dabrowski, M. i Janikowski, L. (2018) *Virtual currencies and their potential impact on financial markets and monetary policy* [online]. Warsaw: Center for Social and Economic Research. Dostupno na: http://www.case-research.eu/files/?id_plik=5708 [15.2.2021.]
8. Draeger, D. D. (2015) *Plus que de l'argent : L'essentiel des bitcoins, des chaînes de blocs et des contrats intelligents* [online]. Canada: Ministère de la Justice. Dostupno na: https://www.justice.gc.ca/fra/pr-rp/jr/bitcoin/bitcoin_fra.pdf [3.3.2021.]
9. Dujella, A. (2003) *Elliptic Curve Digital Signature Algorithm*. Predavanje iz kolegija Eliptičke krivulje i njihova primjena u kriptografiji. Zagreb: Prirodoslovno-matematički fakultet
10. Fantesini, A. (2021). *Digital Euro, advantages and risks of the ECB's new virtual currency* [online]. Rim: Institute for Competitiveness. Dostupno na: <https://www.i-com.it/en/2020/10/16/euro-digitale-bce/> [5.4.2021.]
11. Fernando, J. (2021) *Moving Average* [online]. New York: Investopedia. Dostupno na: <https://www.investopedia.com/terms/m/movingaverage.asp> [21.2.2021.]
12. Fernando, J. (2020) *Relative Strength Index (RSI)* [online]. New York: Investopedia. Dostupno na: <https://www.investopedia.com/terms/r/rsi.asp> [21.2.2021.]

13. Figuet, J.-M. (2016) Bitcoin et blockchain: quelles opportunités? *Revue d'économie financière*, 3 (123) [online]. Dostupno na: <https://www.cairn.info/revue-d-economie-financiere-2016-3-page-325.htm> [3.3.2021.]
14. Giudici, G., Milne, A. i Vinogradov, D. (2020) Cryptocurrencies: market analysis and perspectives. *Journal of Industrial and Business Economics*, 47 (1-18) [online]. Dostupno na: <https://link.springer.com/article/10.1007/s40812-019-00138-6> [18.2.2021.]
15. Hayes, A. (2020) *Bollinger Band® Definition* [online]. New York: Investopedia. Dostupno na: <https://www.investopedia.com/terms/b/bollingerbands.asp> [24.2.2021.]
16. Hayes, A. S. (2017). Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. *Telematics and Informatics* [online], 34 (7) . Dostupno na: <https://www.sciencedirect.com/science/article/abs/pii/S0736585315301118> [17.2.2021.]
17. Higgins, S. (2018) *KFC Canada Is Accepting Bitcoin for Fried Chicke* [online]. New York Francisco: CoinDesk. Dostupno na: <https://www.coindesk.com/kfc-canada-is-accepting-bitcoin-for-fried-chicken> [14.3.2021.]
18. Hrvatska agencija za nadzor financijskih usluga. (2020). *Upravno Vijeće Hanfe izdalo rješenje za osnivanje alternativnog investicijskog fonda za ulaganje u bitcoin* [online]. Zagreb. Dostupno na: <https://www.hanfa.hr/vijesti/upravno-vije%C4%87e-hanfe-izdalo-rje%C5%A1enje-za-osnivanje-alternativnog-investicijskog-fonda-za-ulaganje-u-bitcoin/> [12.3.2021.]
19. Hrvatska narodna banka (2017) *9th Session of the Financial Stability Council* [online]. Zagreb. Dostupno na: <https://www.vfs.hr/en/-/odrzana-9-sjednica-vijeca-za-financijsku-stabilnost> [12.3.2021.]
20. Hrvatska narodna banka (2018) *Što su virtualne valute?* [online]. Zagreb. Dostupno na: <https://www.hnb.hr/-/sto-su-virtualne-valute-> [12.3.2021.]
21. Hossain, S. S., Oni S. S., Mourshed I., Ahmed, R i Islam, T. (2017) *Bitcoins and Its Impact on Financial Markets* [online]. San Francisco: Academia. Dostupno na: https://www.academia.edu/35335525/Bitcoins_and_Its_Impact_on_Financial_Markets [28.2.2021.]
22. Houben, R. i Snyers, A. (2018) *Cryptocurrencies and blockchain* [online]. European Union: Policy Department for Economic, Scientific and Quality of Life Policies. Dostupno na: <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf> [16.2.2021.]
23. Huang, K. i Kim, Y. S. (2006) *A Test of MACD Trading Strategy* [online]. Burnaby: Simon

- Fraser University. Dostupno na: <https://core.ac.uk/download/pdf/56371804.pdf> [2.2.2021.]
24. Ivezić, B. (2018) *Najveći hrvatski ICO skupio 8,1 milijun dolara i ide po još* [online]. Zagreb: Poslovni dnevnik. <https://www.poslovni.hr/kako-su-uspjeli/najveci-hrvatski-ico-skupio-81-milijun-dolara-i-ide-po-jos-343698> [31.3.2021.]
 25. Kuo Chuen, D. L. (2015.) *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Amsterdam: Elsevier Inc.
 26. Landau, J.-P., Genais, A. (2018) *Les crypto-monnaies* [online]. Paris: Ministre de l'Économie et des Finances. Dostupno na: <https://www.vie-publique.fr/sites/default/files/rapport/pdf/184000433.pdf> 17. [28.2.2021.]
 27. Larios-Hernández, G. J. (2017) Blockchain entrepreneurship opportunity in the practices of the unbanked. *Business Horizons* [online], 60 (6). Dostupno na: <https://www.sciencedirect.com/science/article/abs/pii/S0007681317301209#!> [3.3.2021.]
 28. Li, D., Huang, J., Wang, L. (2019) The Impact of Digital Currency on the Financial System: Universal Decentralized Digital Currency, Is It Possible?. *Journal of Economics and Public Finance* [online], 5 (2). Dostupno na: <http://www.scholink.org/ojs/index.php/jepf/article/view/2006> [5.3.2021.]
 29. Ljubaj, I. i L. Martinčević. (2020). *Centralnobankarski digitalni novac – nova moda ili stvarna potreba?* [online]. Zagreb: Hrvatska narodna banka. Dostupno na: <https://www.hnb.hr/-/centralnobankarski-digitalni-novac-nova-moda-ili-stvarna-potreba-#footnote-1> [4.4.2021]
 30. Manning, J. (2017) *How Blockchain Is Changing the Banking Industry* [online]. Dublin: Finance Publishing. Dostupno na: <https://internationalbanker.com/banking/blockchain-changing-banking-industry/> [18.2.2021.]
 31. Magas, J. (2019) *Bitcoin Not Accepted: Burger King's Crypto Foray Short-Lived* [online]. New York: Cointelegraph. Dostupno na: <https://www.businesswire.com/news/home/20200115005482/en/HSB-Survey-Finds-One-Third-Small-Businesses-Accept> [13.3.2021.]
 32. Martucci, B. (2017) *What Is Cryptocurrency – How It Works, History & Bitcoin Alternatives* [online]. Henderson: Money Crashers. Dostupno na: <https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/> [17.2.2021.]
 33. Mikhaylov, A. (2020) Cryptocurrency Market Analysis from the Open Innovation Perspective. *Journal of Open Innovation: Technology, Market, and Complexity* [online], 6 (4). Dostupno na: <https://www.mdpi.com/2199-8531/6/4/197>. [28.2.2021.]
 34. Milewski, D. (2020) *HSB Survey Finds One-Third of Small Businesses Accept*

- Cryptocurrency: Do They Understand the Cyber and Financial Risks?* [online]. San Francisco: Business Wire. Dostupno na: <https://www.businesswire.com/news/home/20200115005482/en/HSB-Survey-Finds-One-Third-Small-Businesses-Accept> [13.3.2021.]
35. Mitchell, C. (2021) *Fibonacci Retracement Levels* [online]. New York: Investopedia. Dostupno na: <https://www.investopedia.com/terms/f/fibonacciretracement.asp> [28.2.2021.]
36. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016) *Bitcoin and Cryptocurrency Technologies* [online]. Princeton: Princeton University. Dostupno na: https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf [5.3.2021.]
37. Narodne novine (2020) *Zakon o sprječavanju pranja novca i financiranja terorizma* [online]. Zagreb: Narodne novine d.d., 39 (19). Dostupno na: <https://www.zakon.hr/z/117/Zakon-o-sprje%C4%8Davanju-pranja-novca-i-financiranju-terorizma> [12.3.2021.]
38. Panetta, F. (2021). Evolution or revolution? The impact of a digital euro on the financial system [online]. Frankfurt na Majni: Europska centralna banka. Dostupno na: <https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210210~a1665d3188.en.html> [5.4.2021.]
39. Porezna uprava (2017) *Porezni tretman kapitalnih dobitaka po osnovi trgovanja kriptovalutama* [online]. Zagreb. Dostupno na: https://www.porezna-uprava.hr/HR_publicacije/Lists/mislenje33/Display.aspx?id=19570 [13.3.2021.]
40. Porezna uprava (2018) *Porezni tretman kapitalnih dobitaka po osnovi trgovanja kriptovalutama* [online]. Zagreb. Dostupno na: https://www.porezna-uprava.hr/HR_publicacije/Lists/mislenje33/Display.aspx?id=19590 [13.3.2021.]
41. Rader, D. (2019) *The Dallas Mavericks Are Now Accepting Bitcoin* [online]. New York: Forbes. Dostupno na: <https://www.forbes.com/sites/doylerader/2019/08/23/the-dallas-mavericks-are-now-accepting-bitcoin/#781a565834b5> [13.3.2021.]
42. Radivojac, G. i Grujić, M. (2019) *Future of cryptocurrencies and blockchain technology in financial markets* [online]. San Francisco: Academia. Dostupno na: https://www.academia.edu/39211850/Future_of_cryptocurrencies_and_blockchain_technology_in_financial_markets [16.2.2021.]
43. Resta, M., Pagnottoni, P., De Giuli, M. E. (2020) Technical Analysis on the Bitcoin Market: Trading Opportunities or Investors' Pitfall?. *Multidisciplinary Digital Publishing Institute* [online], 8 (44). Dostupno na: <https://www.mdpi.com/2227-9091/8/2/44/htm> [4.5.2021.]

44. Tapscott, A. i Tapscott, D. (2017) *How Blockchain Is Changing Finance* [online]. Brighton: Harvard Business Review. Dostupno na: <https://hbr.org/2017/03/how-blockchain-is-changing-finance> [24.4.2021.]
45. The Law Library of Congress (2018) *Regulation of Cryptocurrency Around the World* [online]. Washington: Global Legal Research Center. Dostupno na: <https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf> [22.2.2021.]
46. Yuan, Y. i Wang, F. Y. (2018) Blockchain and cryptocurrencies: Model, techniques, and applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* [online], 48 (9). Dostupno na: <https://ieeexplore.ieee.org/document/8419306> [20.2.2021.]
47. Vlada Republike Hrvatske. (2021). *Ciljni datum uvođenja eura i dalje ostaje 1. siječnja 2023.* [online]. Dostupno na: <https://vlada.gov.hr/vijesti/ciljni-datum-uvodjenja-eura-i-dalje-ostaje-1-sijecnja-2023/31189> [20.4.2021.]

POPIS INTERNETSKIH STRANICA

1. AT&T – službena stranica (2019). *AT&T is the First Mobile Carrier to Accept Payment in Cryptocurrency* [online]. Dallas. Dostupno na: https://about.att.com/story/2019/att_bitpay.html [13.3.2021.]
2. BBC News – službena stranica (2014). *Microsoft to accept payments made in bitcoins* [online]. London. Dostupno na: <https://www.bbc.com/news/technology-30377654> [13.3.2021.]
3. La Patilla – službena stranica (2020). *Burger King Venezuela abre las puertas a las criptomonedas* [online]. Caracas. Dostupno na: <https://www.lapatilla.com/2020/01/02/burger-king-venezuela-abre-las-puertas-a-las-criptomonedas/> [13.3.2021.]
4. Lider Media – službena stranica (2021). *Na 46 benzinskih postaja u Hrvatskoj omogućeno je plaćanje kriptovalutama* [online]. Zagreb. Dostupno na: <https://lider.media/poslovnascena/hrvatska/na-46-benzinskih-postaja-u-hrvatskoj-omoguceno-je-placanje-kriptovalutama-135200> [27.2.2021.]
5. Miami Dolphins – službena stranica (2019). *Litecoin Named Official Cryptocurrency of the Miami Dolphins* [online]. Miami. Dostupno na:

<https://www.miamidolphins.com/news/litecoin-named-official-cryptocurrency-of-the-miami-dolphins> [13.3.2021.]

1. <https://coinmarketcap.com/> [23.6.2021.]
2. <https://litecoin.org/> [15.3.2021.]
3. <https://solarcoin.org/> [15.3.2021.]
4. <https://www.namecoin.org/> [15.3.2021.]
5. <https://musicoin.org/> [15.3.2021.]
6. <https://wepower.com/> [15.3.2021.]
7. <https://www.civic.com/> [15.3.2021.]
8. <https://www.billpayforcoins.com/index.php> [13.3.2021.]
9. <https://coinatmradar.com/> [27.2.2021.]
10. <https://coinmap.org/> [13.3.2021.]
11. <https://www.tap.global/> [13.3.2021.]
12. <https://bitpay.com/> [13.3.2021.]
13. https://donate.wikimedia.org/wiki/Ways_to_Give [13.3.2021.]
14. <https://archive.org/donate/cryptocurrency/> [13.3.2021.]
15. <https://purse.io/shop> [13.3.2021.]
16. <https://www.tradingview.com> [14.2.2021.]
17. <https://electrocoin.hr/> [20.3.2021.]
18. <https://www.griffon-am.hr/> [20.3.2021.]
19. <https://www.dapowerplay.com/> [20.3.2021.]
20. <https://www.idejanakvadrat.hr/> [20.3.2021.]
21. <https://fimaplus.com/> [20.3.2021.]
22. <https://tolar.io/tokensale#token-metrics> [20.3.2021.]
23. <https://www.cryptocompare.com> [4.5.2021.]

POPIS SLIKA

Slika 1. Uvjeti bitcoin rudarenja	4
Slika 2. Kriteriji valjanosti bloka	7
Slika 3. <i>Hash</i> pokazivači u blockchainu	11
Slika 4. Otkrivanje neovlaštenih mijenjanja informacija <i>hash</i> pokazivačima	11
Slika 5. Notacija i QR kôd	14

POPIS TABLICA

Tablica 1. Kriptovalute prema tržišnoj kapitalizaciji	22
---	----

POPIS GRAFIKONA

Grafikon 1. Smanjenje nagrade za rudarenje nakon svakog 210.000. bloka	5
Grafikon 2. Ukupna tržišna kapitalizacija kriptovaluta od 1. prosinca 2017. do 1. siječnja 2021.	20
Grafikon 3. Udio u tržištu kriptovaluta u %	22
Grafikon 4. Indeks relativne snage	37
Grafikon 5. Bollingerove ovojnice	38
Grafikon 6. Primjer Fibonnacijevih razina na tečaju bitcoin/dolar	40
Grafikon 7. Jednostavni pomični prosjek	42
Grafikon 8. Eksponecijalni pomični prosjek	43

ŽIVOTOPIS

Marcela-Maria Skrbín rođena je 8. ožujka 1996. godine u Sisku. Osnovnu školu završila je 2011. godine, nakon čega upisuje Opću gimnaziju u Sisku. Maturirala je 2015. godine te iste godine upisuje Integrirani preddiplomski i diplomski sveučilišni studij Poslovna ekonomija na Ekonomskom fakultetu u Zagrebu. 2018. godine odabire smjer Financije.

Aktivno koristi engleski, francuski i njemački jezik, a pasivno talijanski, španjolski, kineski, japanski i ruski jezik. Od digitalnih vještina koje posjeduje ističe se odlično upravljanje Microsoft Office paketom te dobro poznavanje programskih jezika C, C#, CSS, HTML te JavaScript.

Za vrijeme studija bila je demonstratorica na Katedri za Informatiku na kolegijima Informatika, Poslovni informacijski sustavi, Sustavi upravljanja poslovnim procesima te Poslovni informacijski sustavi.

Dobitnica je stipendije Francuske ambasade 2019. godine, a 2021. godine dobitnica je stipendije njemačke pokrajine Bavarske.