Digitalne valute kao novi sigurnosni izazov država EU

Maleš, Neven

Professional thesis / Završni specijalistički

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, The Faculty of Political Science / Sveučilište u Zagrebu, Fakultet političkih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:114:867826

Sveučilište u Zagrebu
Fakultet političkih znanosti
Poslijediplomski sveučilišni
specijalistički studij Sigurnosna politika RH

Ime i prezime studenta: NEVEN MALEŠ

DIGITALNE VALUTE KAO NOVI SIGURNOSNI IZAZOV DRŽAVA EU

ZAVRŠNI SPECIJALISTIČKI RAD

Zagreb, listopada 2023.

Sveučilište u Zagrebu
Fakultet političkih znanosti
Poslijediplomski sveučilišni
specijalistički studij Sigurnosna politika RH

Ime i prezime studenta: NEVEN MALEŠ

DIGITALNE VALUTE KAO NOVI SIGURNOSNI IZAZOV DRŽAVA EU

ZAVRŠNI SPECIJALISTIČKI RAD

Mentor: prof.dr.sc. Siniša Tatalović

Student: Neven Maleš

Zagreb, listopada 2023.

Izjavljujem da samo završni specijalistički rad Digitalne valute kao novi sigurnosni izazov, koji sam predao na ocjenu mentoru dr.sc.prof. Siniši Tatalović, napisao samostalno i da je u potpunosti riječ o mojem autorskom radu. Također, izjavljujem da dotični rad nije objavljen ni korišten u svrhe ispunjenja nastavnih obveza na ovom ili nekom drugom učilištu, te da na temelju njega nisam stekao ECTS bodove.

Nadalje, izjavljujem da sam u radu poštivao etička pravila znanstvenog i akademskog rada, a posebno članke 16-19. Etičkoga kodeksa Sveučilišta u Zagrebu.

Neven Maleš

SADRŽAJ RADA:

POPIS ILUSTRACIJA:

SAŽETAK

Pojavom blockchain tehnologije i digitalnog transakcijskog sustava Bitcoin, započela je nova era u modernom monetarnom svjetskom sustavu. Otpornost, sigurnost i anonimnost koje je ovakav sustav pružio, otvorili su vrata za brojne nove primjene te unapređenja postojećih sustava plaćanja. Sa tehničkim napretkom i značajkom anonimnosti došlo je do pojave korištenja ovog revolucionarnog sustava u kriminalne svrhe. Sigurnosni rizici koje je uvjetovala upotreba digitalnih valuta su korištenje digitalnih valuta u kriminalne svrhe, nezakonitu trgovinu, financiranje terorizma, izbjegavanje poreza i transfera vrijednosti. Države u kojima je korištenje digitalnih valuta popularizirano odlučuju se za potpunu zabranu ili reguliranje tržišta digitalnih valuta. Primjer potpune zabrane je Kina dok je primjer slojevite i izrazito kompleksne regulative SAD. EU kasni sa prepoznavanjem digitalnih valuta kao sredstva i infrastrukture za transfer vrijednosti. Regulativni okvir u EU je relativno nov te koristi samo dio tehnologije i alata nadzora koju koristi SAD. Pravilno definiranje pojma digitalnih valuta te kreiranje sveobuhvatne sigurnosne politike sukladno političkom uređenju i ekonomskom stanju države je od presudne važnosti. Potpuni nadzor nad transferom i trgovinom digitalnim valutama još nije moguć radi visoke razine anonimnosti mrežnih transakcija te su se države odlučile na kontrolu ulaska i izlaska kapitala na mrežu regulacijom centraliziranih mjenjačnica.

1. UVOD

Težnja čovjeka ka proizvodnji nove vrijednosti je univerzalna i svevremenska. Prelaskom na sjedilački način života, nastankom gradova te naprednijih načina proizvodnje hrane i alata, dolazi i do ekspanzije trgovine. Robna razmjena kao teoretski najjednostavniji način razmjene vrijednosti nije bio primjenjiv na visokoj razini trgovine. Razvoj trgovine pratio je i razvoj novčanih valuta i transakcija vrijednosti. Transakcija novca je aktivnost između dvije ili više strana, kojoj je cilj transfer vrijednosti na što brži, sigurniji i jednostavniji način sa što manje troškova. Kako bi se navedeni uvjeti mogli ispuniti bile su potrebne centralne institucije, koje bi nadzorom nad tokom novčanih sredstava i primjenom zakona i pravila osigurale sigurno okruženje u sektoru plaćanja. Razvojem slobodnog društva rodila se želja za nenadziranim, sigurnim i autonomnim sustavom plaćanja u kojem bi mogao sudjelovati bilo koji korisnik bez obzira na geografski položaj ili valutu države u kojoj se nalazi. Ovakav sustav morao je biti otporan na pokušaj cenzure, zabrane ili hakerskih napada trećih strana, što je uvjetovalo zahtjev za distribuiranom arhitekturom sustava plaćanja i dovoljnu razinu anonimnosti njegovih korisnika. Pojavom blockchain tehnologije i digitalnog transakcijskog sustava Bitcoin, započela je nova era u modernom monetarnom svjetskom sustavu. Otpornost, sigurnost i anonimnost koje je ovakav sustav pružio, otvorili su vrata za brojne nove primjene te unapređenja postojećih sustava plaćanja. Sa tehničkim napretkom i značajkom anonimnosti došlo je do pojave korištenja ovog revolucionarnog sustava u kriminalne svrhe. Trgovina nedozvoljenim proizvodima, pranje novca, financiranje terorističkih organizacija, prevare, destabilizacija monetarnog sustava i drugi rizici potaknuli su, prvenstveno institucije SAD-a, u kreiranju opsežnog regulativnog okvira za čiju je operacionalizaciju zaduženo nekoliko različitih financijskih i sigurnosnih agencija.

Pojavom blockchain tehnologije, napadi na ekonomsku i društvenu stabilnost, te samim time i sigurnost države, društva i pojedinca, su otvorili potpuno novo bojište za koje je trebalo pripremiti zakonodavnu i operativnu pozadinu. Unatoč relativno brzoj prilagodbi novim sigurnosnim izazovima od strane regulativnih organizacija i sigurnosnih agencija SAD-a gdje je još nejasno određena podjela odgovornosti utjecala na preklapanje rada više agencija i tijela, Europska Unija je primijenila blaži pristup te je relativno kasnije okarakterizirala novonastale okolnosti kao potencijalne sigurnosne izazove te je i sam proces prilagodbe istima nešto kasnije započeo.

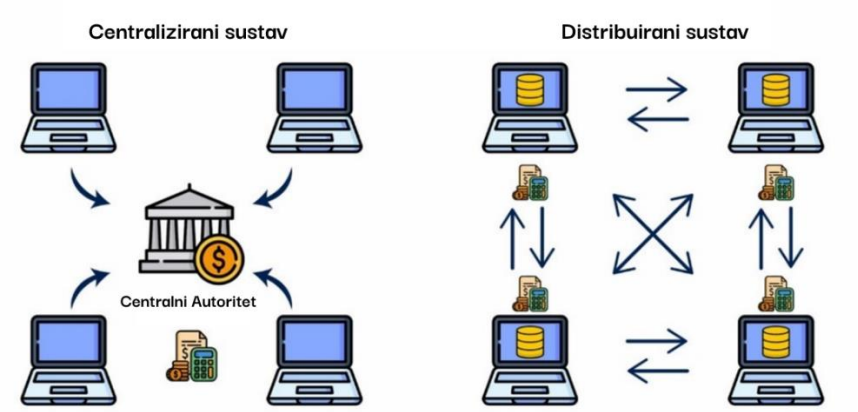
Trenutna literatura koja se bavi sigurnosnim izazovima koje predstavljaju digitalne valute te regulatornim odgovorima pojedinih država je ograničena, te se većina autora bazira na obradi problema uvođenja digitalne valute centralnih banaka te temom kriminalnih aktivnosti uvjetovanih pojava digitalnih valuta. Ovaj rad obrađuje nove sigurnosne izazove koji su nastali pojavom blochchaina te regulativnu prilagodbu zemalja Europske Unije. Glavno istraživačko pitanje bavi se procesom prilagodbe EU novim izazovima i prijetnjama koje predstavlja blockchain te načinom na koji je provedena prilagodba sigurnosnih sustava. S obzirom da se monetarna tijela država poput EU i Rusije već nekoliko godina pripremaju na uvođenje digitalnih valuta centralnih banaka, od iznimne je važnosti odgovoriti na istraživačko pitanje ovog rada. Da bi se dobio konkretan i sveobuhvatan odgovor, napravljen je povijesni pregled nastanka i razvoja blockchain tehnologije te tehničke karakteristike koje ovu tehnologiju čine posebnom u odnosu na tradicionalne transakcijske sustave. Nakon upoznavanja sa povijesnom pozadinom te tehničkim karakteristikama, prikazan je pregled svih prijetnji i novonastalih, potencijalno štetnih pojava koje donosi blockchain. Modeli prilagodbe država poput SAD-a, Kine i Rusije su obrađeni nakon ove cjelokupne uvertire u problematiku blockchaina te je izvršena usporedba prilagodbe SAD-a i EU-a kao dvije krajnosti po pitanju rigoroznosti te operativne primjene regulativnog okvira. Ovaj rad se dotaknuo i procesom prilagodbe blockchain tehnologiji sigurnosnih tijela u RH, te prikazao trenutnu poziciju istih u odnosu na SAD i EU.

Razmjeri štete prouzročene kriminalnim aktivnostima te rastuća popularnost digitalnih valuta jasno upućuju da je regulacija tržišta neizbježna. Komponente sigurnosnog sustava država koje su uvele regulacije ili u potpunosti zabranile digitalne valute, sadrže sva relevantna tijela financijskog nadzora te tradicionalne agencije za istragu i primjenu zakona. Borba za kontrolu tržišta digitalnih valuta jasno potvrđuje tezu kako je sigurnost u modernom svijetu sveobuhvatna, dinamična djelatnost u kojoj moraju sudjelovati svi elementi, od pojedinca do globalnih organizacija. EU je samo djelomično uspjela u svom naumu da ostvari kontrolu nad financijskim sustavom, te je opsežnu zakonodavnu pozadinu potrebno poduprijeti operativnim tijelima koje će imati sposobnost prikupljanja podataka, analize te primjene alata za izvršavanje zakonodavnih pravila. Politika minimaliziranja utjecaja na razvoj blockchain tehnologija pri uvođenju novih zakonodavnih i operativnih pravila, utjecala je na slabiji nadzor i operacionalizaciju sigurnosnih tijela u EU.

2. POVIJEST DIGITALNIH VALUTA

Tehnologija koja je omogućila razvoj digitalnih valuta je takozvana „Blockchain“ tehnologija. Blockchain tehnologija se zasniva na Digital Ledger, odnosno tehnologiji digitalne knjige koja omogućuje stvaranje dijeljene, sinhronizirane i konsenzusno upravljane aktivne baze podataka. Ovakva baza podataka, uz ispunjavanje određenih infrastrukturnih uvjeta, nudi alternativu za mnoge centralizirane, tradicionalne baze podataka i sustave. Centralizirane sustave uglavnom možemo okarakterizirati kao najoptimalnije u pogledu performansi, no s puno nižom razinom sigurnosti radi svoje centralizirane strukture koja zahtijeva postojanje centralne administracijske komponente koja predstavljaju sistemski rizik u jednoj točki - odnosno „single point of failure“ (SPOF). Ukoliko je sigurnost ili pouzdanost SPOF komponente kompromitirana, cijeli sustav je kompromitiran, što u financijskim sustavima može predstavljati ogroman rizik.

Slika 1: Razlika između centraliziranog i distribuiranog transakcijskog sustava



Izvor: https://blog.svcapital.io/difference-between-blockchain-and-distributed-ledger/

2.1. Prva faza razvoja: 1982.-2009.

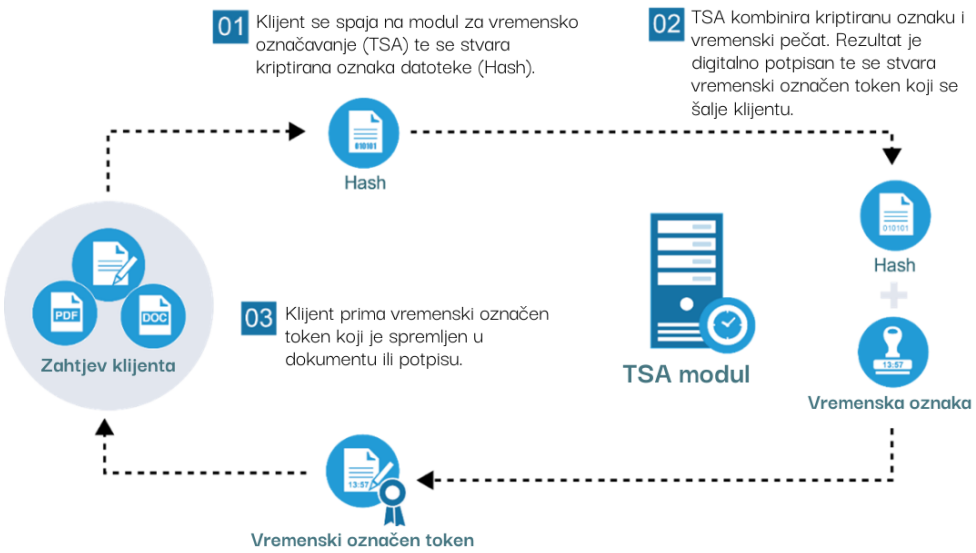
Upravo ideja o kreiranju decentralizirane baze podataka koja bi mogla skladištiti i verificirati vjerodostojnost podataka bez centralne administracijske komponente je inspirirala Davida Chauma, američkog kompjuterskog inženjera, kriptografa i izumitelja da u svojoj dizertaciji iz 1982. godine „Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups“ prvi put spomene pojam „Blockchain“. Centralna teza Chaumove dizertacije je da „Organizacije koje ne vjeruju jedna drugoj mogu izgraditi i održavati visoko siguran računalni sustav za verifikaciju i pohranu podataka kojem svi

sudionici mogu vjerovati“ (Chaum, 1982: 5). Kao primjer primjene njegovog nacrta Blockchaina, Chaum prvenstveno navodi financijske sustave kao što su Federal Reserve Bank of America, IRS te bankarske sustave, ne ograničavajući primjenu i u drugim sektorima kao što su servisi javnog zdravstva, edukacijskog sustava, osiguravateljskih kuća te vojske. Njegova vizija Blockchain tehnologije je sadržavala gotovo sve komponente današnje tehnologije koja se koristi za verifikaciju transakcija modernih digitalnih valuta kao što su Bitcoin, Ethereum i druge. Razliku između Chaumovog sustava i blockchaina kojeg koriste moderne digitalne valute ćemo obraditi u sljedećem poglavlju.

Chaumova ideja je zaintrigirala znanstvenu zajednicu koja je pomoću njegovog nacrta blockchain tehnologije pokušavala pronaći jedinstveno rješenje za rješavanje problema poput neovlaštene izmjene digitalnih dokumenata. Nemoguće je bilo graditi pouzdane sustave financijskih transakcija bez tehnologije koja bi omogućila vjerodostojni prikaz i nadzor nad sigurnošću verifikacijskog procesa te podatke o samoj transakciji i vremenskom periodu u kojem je transakcija izvedena.

U svojoj disertaciji „How to Time-Stamp a Digital Document“ Stuart Haber i W. Scott Stornetta predlažu rješenje za vremensko označavanje digitalnih dokumenata čime bi se, u nekom budućem informacijskom sustavu, osigurala neprekidnost zapisa vremenskih procesa odnosno utvrdilo koji informacijski zapis se dogodio prije, a koji poslije. U ovoj disertaciji autori predlažu „računalne praktične postupke za digitalno vremensko označavanje takvih dokumenata da je korisniku nemoguće svojevoljno datirati svoj dokument unatrag ili unaprijed“ (Haber, Stornetta 1991: 7). Za ostvarivanje ove teze autori smatraju da je potrebno zadovoljiti dva uvjeta: „Prvo, mora se pronaći način da se samim podacima doda vremenski žig, bez ikakvog oslanjanja na karakteristike podataka medija na kojem se podaci pojavljuju, tako da je nemoguće promijeniti i jedan dio dokumenta ,a da promjena nije vidljiva. Drugo, trebalo bi biti nemoguće ovjeriti dokument, a da su vrijeme i datum drugačiji od stvarnog.“ (Haber, Stornetta 1991: 8).

Slika 2: Primjer centraliziranog (TSA) vremenskog označavanja digitalne informacije

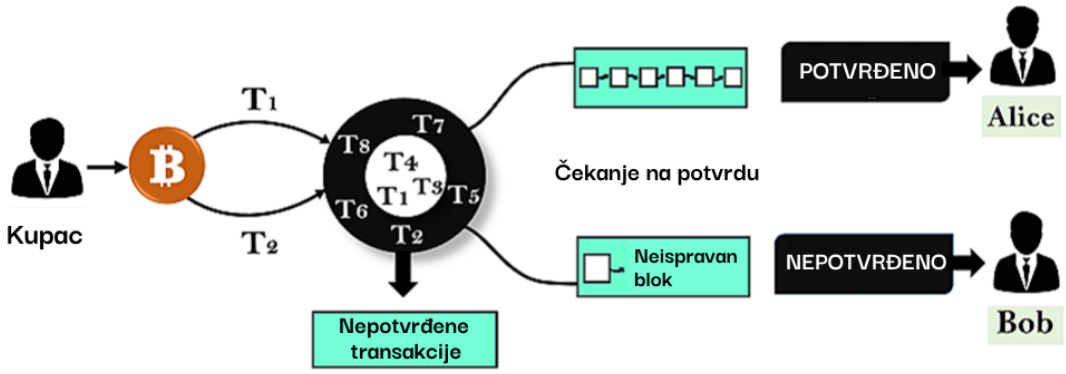


Izvor: https://www.globalsign.com/en/blog/what-is-timestamping-how-does-it-work

Autori predlažu dva rješenja, centralizirano i decentralizirano, od kojih se ovo posljednje implementiralo te pridonijelo daljnjem razvoju blockchain tehnologije. U primjeni ovog rješenja, nekoliko članova skupine korisnika određenog informacijskog sustava mora staviti vremensku oznaku na kriptiranu informaciju zvanu „hash“. Članovi koji verificiraju transakciju se biraju pomoću pseudo-slučajnog generatora koji koristi „hash“ samog dokumenta kao početnu vrijednost što je vrlo važna značajka budućih decentraliziranih financijskih sustava – potpuna decentraliziranost i nasumičnost verifikacija transakcijskog procesa.

U 1998. godini Nicholas Szabo, računalni znanstvenik i kriptograf, dizajnira decentraliziranu digitalnu valutu Bit Gold koja nikad nije zaživjela u blockchain svijetu, ali je bila izravna preteča arhitekturi Bitcoina. Ova iteracija blockchaina je zahtijevala računalnu snagu, osiguranu od strane korisnika mreže, za rješavanje kriptografskog zadatka kojim bi se verificiralo prethodni i trenutni informacijski blok. Svaki novi blok bi se dodao na lanac blokova sukladno vremenskom redoslijedu u kojem je blok nastao. Ovakav sustav je objedinio dotadašnja saznanja o blockchain tehnologiji i kreirao sustav kojim je bilo moguće decentralizirano verificirati i vremenski označiti određenu informaciju – transakciju. Iako nije praktično isproban, Szabin sustav je riješio problem dvostrukog plaćanja, koji je u to doba bio relativno česta pojava u sustavima digitalnog novca, gdje bi se radi nepostojanja vremenske značajke informacije, isti digitalni token mogao potrošiti više od jednog puta.

Slika 3. Rješenje problema dvostrukog plaćanja korištenjem blochchaina



Slika 3. Rješenje problema dvostrukog plaćanja korištenjem blochchaina

Izvor: https://www.javatpoint.com/blockchain-double-spending

2.2 Prva praktična primjena - Bitcoin

Prva i najpoznatija praktična primjena blockchain tehnologije je konceptualizirana od strane jedne ili više osoba, koje su pod pseudonimom Satoshi Nakamoto 2008. godine predstavili poboljšanu verziju dotadašnjeg blockchaina u bijeloj knjizi – „Bitcoin: A Peer-to-Peer Electronic Cash System“. Glavne značajke Nakamotovog doprinosa razvoju blockchaina je vremensko označavanje informacijskog bloka bez korištenja treće strane – značajka koja je u potpunosti decentralizirala sve komponente blockchain tehnologije. Također, Nakamoto je uveo parametar kompleksnosti čime je stabilizirao brzinu nastanka novih informacijskih blokova. Konačno, 09. siječnja 2009. godine, Nakamoto je pokrenio prvu decentraliziranu transakcijsku mrežu – Bitcoin, čime je započeo financijsku revoluciju koja polako, ali sigurno preuzima sve veći dio financijskih tržišta. Zanimljiva činjenica je da je u prvom informacijskom bloku Nakamoto ugradio tekst novinskog naslova The Timesa - "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks", što se može interpretirati kao način vremenskog označavanja, ali i kao komentar na nestabilnost mehanizma frakcionalnih rezervi korištenog u bankarskim sustavima. Bitcoin je i danas najpoznatija digitalna valuta sa najvećim udjelom tržišta koji se u zadnjih 5 godina kreće od 45 do 70% ukupnog tržišta digitalnih valuta (Coingecko 2022.). Do 2017. godine tržišni udjel Bitcoina je iznosio više od 95% ukupnog tržišta (Slika 4.), što govori o dominaciji istog, ali i upućuje na sljedeću fazu

razvoja blockchain tehnologije koja je iznjedrila tehnološki naprednije digitalne valute i mreže koje polako preuzimaju sve veći dio tržišta.

Slika 4. Udjel Bitcoina u tržištu digitalnih valuta (2015.-2022.)

Izvor: https://www.tradingview.com/symbols/CRYPTOCAP-BTC.D/

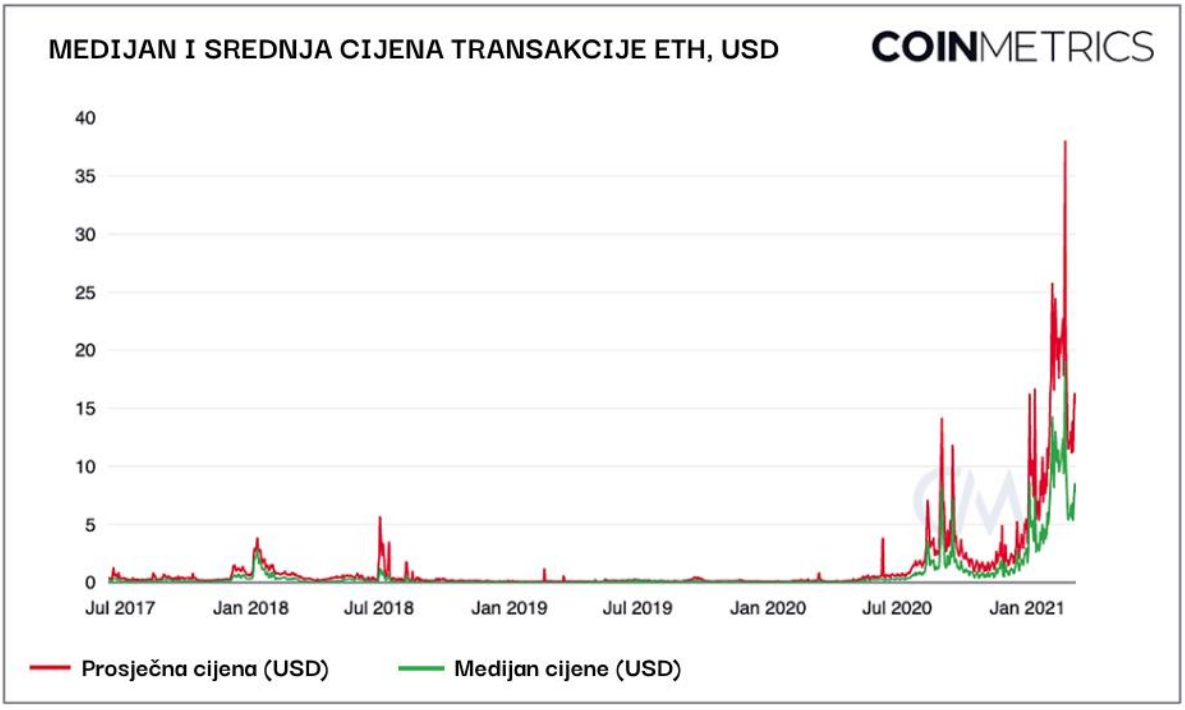
2.3 Druga faza razvoja – Pametni ugovori (2013.-2018.)

Nedostaci blockchain tehnologije Bitcoina potaknuli su programere Vitalika Buterina, Gavina Wooda, Charlesa Hoskinsona, Anthonija Di Loria i Josepha Lubina u razvijanju nove decentralizirane mreže za transakcije digitalnih valuta – Ethereum. Koncept je dizajniran u 2013. godini, a mreža je pokrenuta 2015. godine te je radi jedinstvenih karakteristika ovaj napredak u razvoju digitalnih valuta prozvan Blockchain 2.0. Glavna razlika između Ethereuma i Bitcoina, osim mehanizma koncenzusa, koji za ovaj rad nije od posebne važnosti, je u tome što se Ethereum mreža može koristiti za niz aktivnosti i aplikacija, za razliku od Bitcoina koji je isključivo transakcijska mreža. Ethereum je omogućio postavljanje pametnih ugovora (eng. Smart Contracts) na blockchain mrežu čime je otvoren put za razvoj Decentraliziranih Financija (DeFi). DeFi predstavlja decentralizirano financijsko tržište koje koristi automatizirane aplikacije postavljene na blockchain mrežu, koje bez centralnog poslužitelja ili administratora provode određene mehanizme čiji je ishod određen uvjetima ugovora koje stranke digitalno potpisuju. Ovaj izum je uvjetovao snažnu ekspanziju tržišta digitalnih valuta s obzirom da su tradicionalni financijski akteri uvidjeli snažnu fundamentalnu

vrijednost koju predstavljaju financijske aplikacije postavljene na decentralizirane mreže. Anonimnost, decentraliziranost, transparentnost i jednostavnost korištenja koju je pojava Ethereuma, DeFI-ja i Blockchaina 2.0 omogućila, predstavljala je ne samo revoluciju u financijskim mehanizmima i sustavima, već i društveni pokret koji se zalagao za navedene značajke nasuprot tradicionalnih bankarskih proizvoda i monetarnih sustava.

Ethereum mreža je u stalnom procesu nadogradnje i razvijanja kako bi se korisnicima pružilo besprijekorno iskustvo korištenja decentraliziranih aplikacija. Iako je trenutno mreža koja je najbliže idealu koji je predstavljen kombinacijom decentralizacije, sigurnosti i skalabilnosti, Ethereum mreža nije savršena. To je i dokazano tijekom perioda u kojima je mreža bila korištena intenzivnije kao što je 2018. i pogotovo 2021. godina – godine u kojima je tržište digitalnih valuta ostvarilo nagli rast cijena, tržišnih udjela i broja korisnika. Jedan od glavnih problema Ethereum mreže koji se još uvijek pokušava riješiti je skalabilnost – pri velikom broju transakcija koje mreža treba odraditi, cijena pojedinačne transakcije ima tendenciju rasta, što u krajnjim slučajevima kada je mreža „zagušena“ može dovesti do neodrživih cijena transakcija (Slika 5.) i samim time do neupotrebljivosti mreže, pogotovo za manje transakcije.

Slika 5. Povijesni prikaz cijena transackcije na Ethereum mreži



Izvor: https://coinmetrics.io/

2.4 Treća faza razvoja – Blockchain 3.0 (2018.- danas)

Povijest i evolucija blockchaina ne prestaje s Ethereumom i Bitcoinom. Posljednjih godina niz projekata je otkrilo nove mogućnosti iskorištavanja blockchain tehnologije. Novi projekti nastojali su riješiti neke od nedostataka Bitcoina i Ethereuma dok su osmišljavali nove značajke koje iskorištavaju mogućnosti blockchaina. Glavna značajka 3. faze razvoja blockchaina je ta što se ova tehnologija počinje koristiti u sustavima koji nisu namijenjeni isključivo financijskim aplikacijama.

Gore razmotrena povijest blockchaina uključuje javne blockchain mreže, gdje svatko može pristupiti sadržaju mreže. Međutim, s razvojem tehnologije, mnoge su tvrtke počele interno usvajati ovu tehnologiju kao način povećanja operativne učinkovitosti. Velike tvrtke ulažu sredstva u zapošljavanje stručnjaka jer žele steći prednost u korištenju tehnologije te su tvrtke poput Microsofta preuzele vodstvo kada je riječ o istraživanju primjene blockchaina što je rezultiralo onim što je postalo poznato kao privatni, hibridni i unificirani blockchain.

Također, razvoj blockchaina je zadnjih godina omogućio i interoperabilnost među zasebnim mrežama putem IBC (Inter - Blockchain Communication) protokola, kojim se informacije mogu slati među mrežama bez narušavanja sigurnosti. Primjer projekta koji koristi IBC je Cosmos (ATOM). U ovoj fazi razvoja blockchaina pojavile su se i nove, naprednije mreže, takozvane „Ethereum killers“, kao što je Solana i Avalanche, koje omogućuju procesuiranje više tisuća transakcija u sekundi. Za usporedbu VISA je sposobna obraditi do 24,000 transakcija u sekundi (trenutni prosjek je 1700), Bitcoin 7, a Ethereum ~20 (Slika 6.). S obzirom da se Ethereum mreža, koja je i dalje najpopularnija mreža DeFI-ja, nastavlja razvijati, inovator Vitalik Buterin smatra da sa najnovijim poboljšanjem mreže Ethereum (Ethereum 2.0) može doseći i do 100.000 transakcija u sekundi.

Slika 6: Prikaz broja transackcija vodećih mreža za digitalne transakcije i VISA-e

Izvor: https://blog.kaiko.com/scaling-ethereum-the-role-of-rollups-8e8229f662a4

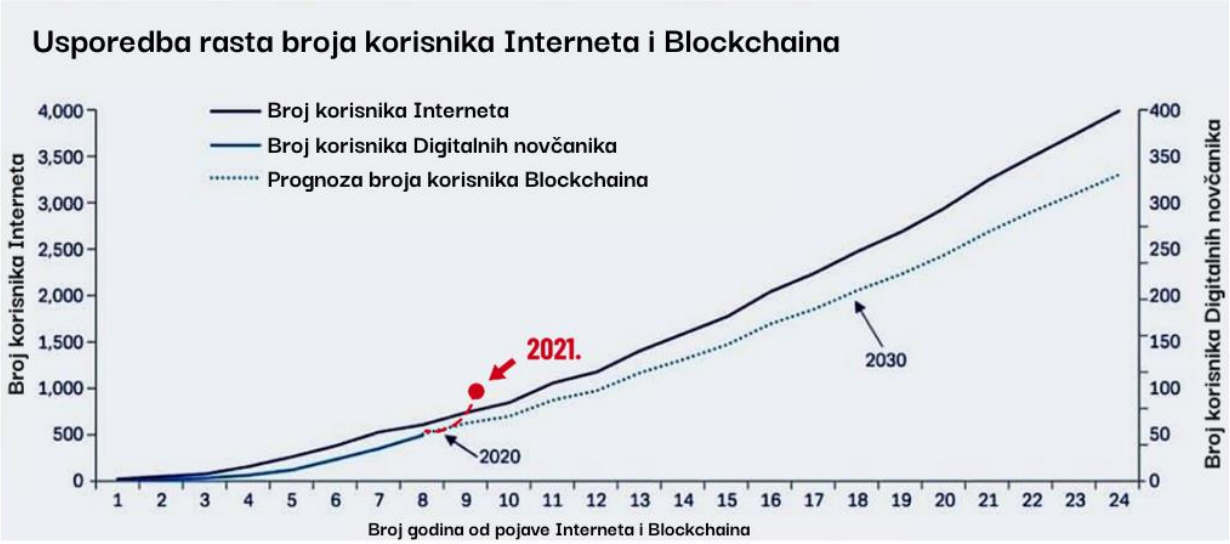
Moderne blockchain mreže kao što je Monero, stvorene su kao način rješavanja problema sigurnosti i skalabilnosti povezanih s ranim aplikacijama blockchaina. Ove vrste mreža, koje pripadaju u klasu „Privacy Altcoins“, imaju za cilj pružiti visoku razinu privatnosti i sigurnosti kada je riječ o transakcijama. Naravno, anonimnost je značajka koja može biti upotrebljena u dobre i loše svrhe te je Monero danas poznat i kao najpopularnija blockchain mreža za plaćanja u kriminalnim aktivnostima kao što su trgovina drogom, oružjem te ostalim plaćanjima na crnom internetu (eng.darkweb).

Razvoj blockchaina je još uvijek u ranoj fazi te su financijski mehanizmi i arhitektura pojedinih projekata podložni hakerskim napadima i/ili financijskim malverzacijama. Najpoznatiji primjer loše dizajniranog projekta je Terra – LUNA koji je u 2022. godini radi lošeg dizajna mehanizma izdavanja svog algoritamskog „dolarskog“ tokena (eng. stablecoin) izgubio 99.99% vrijednosti odnosno više od 40 milijardi dolara izravne štete vlasnicima digitalnog tokena (NY Times 2022.). Neizravna šteta za tržište je neprocjenjiva radi velikog broja likvidacija LUNA/UST pozicija koje su korištene kao pokriće za pozajmice mnogih kompanija za ulaganje u digitalne tokene.

Unatoč greškama u dizajnu, hakerskim napadima te čestim malverzacijama osnivača projekata, broj korisnika blockchain tehnologije i digitalnih tokena neprestano raste. Često se za usporedbu uzima krivulja rasta broja korisnika Interneta koju je do 9.-te godine od puštanja u javnost identično pratila i krivulja rasta broja korisnika blockchaina. Ipak, izvješće Crypto.com-a za siječanj 2021. godine pokazala je brojku od 106 milijuna korisnika

blockchaina, što je pokazalo agresivniji rast broja blockchaina nego što je to bio rast Internet korisnika (Slika 7.), što je i razumljivo uzimajući u obzir da je broj korisnika Interneta preduvjet i snažan katalizator za korištenje blockchaina.

Slika 7: Usporedba rasta broja korisnika Interneta i blockchain tehnologija



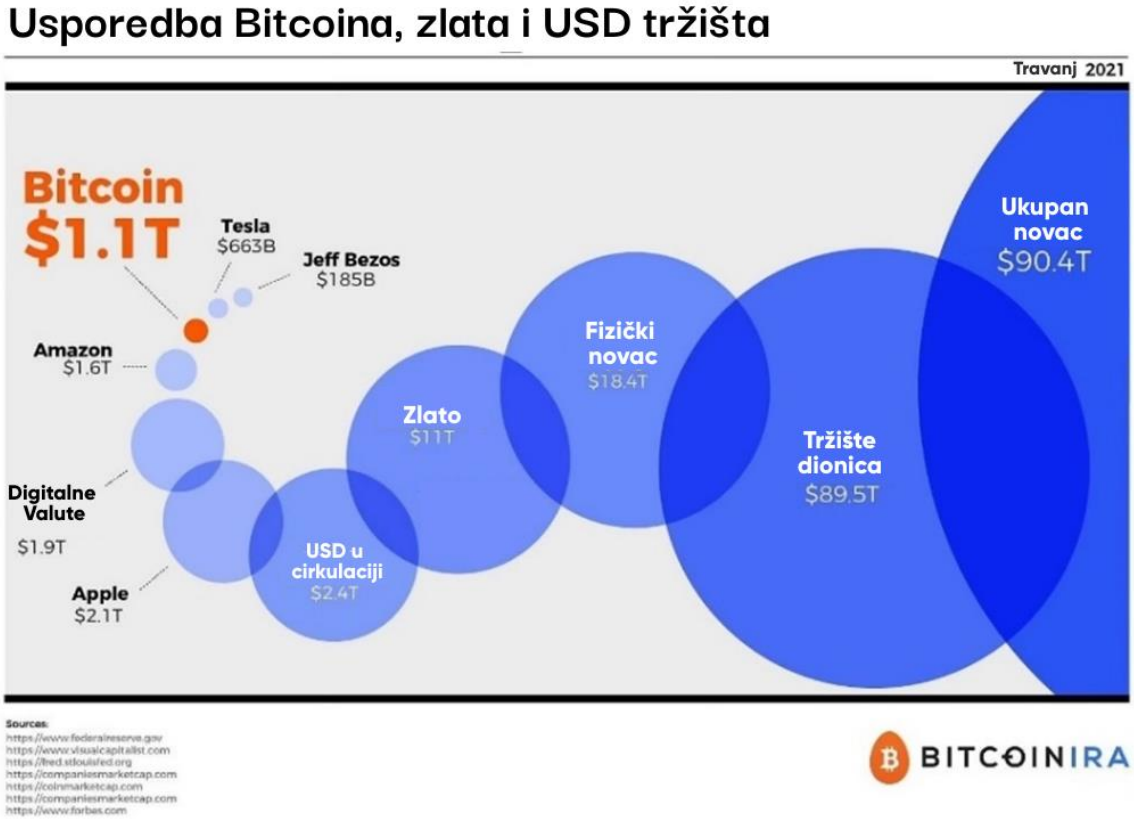
Izvor: Deutsche Bank

Trenutna ukupna vrijednost tržišta digitalnih valute se kreće oko 1000 milijardi dolara ($1T) (Coingecko 2022.), s jakom tendencijom rasta, kako u smislu vrijednosti naspram dolara tako i u rastu broja korisnika. Veći broj korisnika uvjetuje i veći broj prevara, hakerskih napada, eksploatacija te ostalih sigurnosnih rizika kao što su financiranje terorizma i organiziranog kriminala te financijskih rizika koji mogu prouzrokovati nestabilnost na ostalim tržištima ukoliko tržište digitalnih valuta u narednim godinama nastavi ostvarivati dosadašnju stopu rasta. Upravo zato su vlade vodećih svjetskih ekonomija prepoznale tržište digitalnih valuta kao financijski sektor za koji je potrebno stvoriti regulativni okvir te instrumente za provođenje istog.

Slika 8: Kretanje vrijednosti tržišta i količine prometa digitalnih valuta 2014.-2022. godina

Izvor: coinmarketcap.com

Slika 9: Usporedba veličine glavnih financijskih tržišta i tržišta digitalnih valuta (travanj 2021.)



Izvor: bitcoinira.com

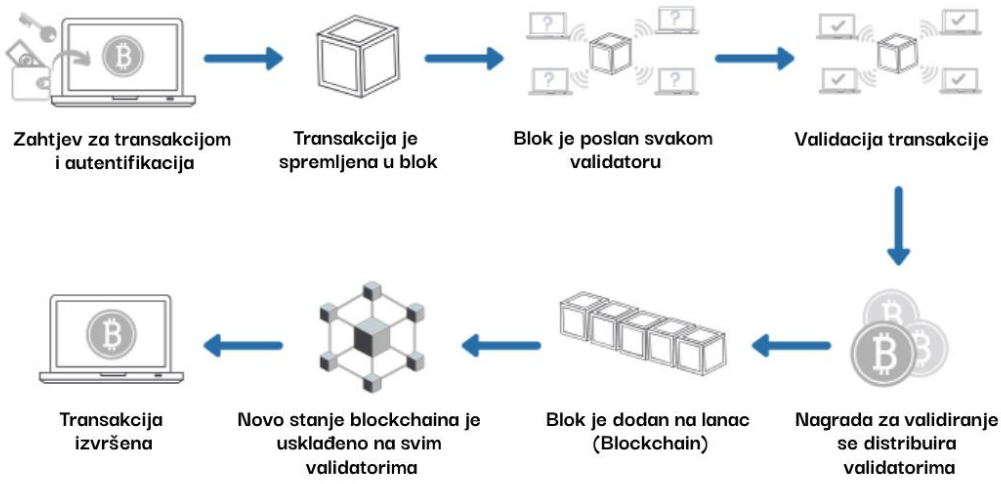
3. ZNAČAJKE BLOCKCHAIN TEHNOLOGIJE

Kako bi razumjeli doseg novih tehnoloških mogućnosti koju donosi pojava Blockchain tehnologije te uzročno posljedičnu povezanost sa ugrozama i rizicima koji proizlaze iz iste, nužno je poznavati tehnički opis modela Blockchaina, te koje prednosti i nedostatke ova tehnologija pruža u odnosu na tradicionalne transakcijske sustave. Funkciju i opis modela blockchaina najjednostavnije možemo prikazati na primjeru Bitcoina, transakcijskog digitalnog „kripto“ sustava koji predstavlja prvu i najpoznatiju operativnu izvedbu dotadašnjih teoretskih dostignuća na polju blockchain tehnologije. Iako je tijekom posljednjeg desetljeća izumljeno više blockchain transakcijskih mrežnih sustava koji su po tehničkim karakteristikama napredniji, te po određenim strukturnim elementima drugačiji od Bitcoina, operativni mehanizmi se baziraju na istim fundamentalnim načelima, stoga je za potrebe ovog rada sasvim zadovoljavajuće promatrati i analizirati blockchain model kroz Bitcoinovu izvedbu istoga.

3.1 Tehnički opis Bitcoin modela Blockchaina

Bitcoin je decentralizirani digitalni sustav plaćanja (transakcija) izumljen od strane jednog ili više inženjera pod pseudonimom Satoshi Nakamoto. Baziran je na principu „peer to peer“ (P2P) mreže i probabilističkog distribuiranog koncenzusnog protokola. Za razliku od centraliziranih sustava koji koriste banke, svaka transakcija na Bitcoin mreži je zapisana, verificirana i sačuvana od strane decentraliziranog sustava kojeg tvore „validatori“ ili takozvani „rudari“. „Validator“ je član mreže koji svoju računalnu snagu koristi za rješavanje kriptografskih problema čime potvrđuje određenu transakciju. Konkretno, nakon što se generira određena količina zahtjeva za transakcije, iste se „pakiraju“ tvoreći blok. Taj blok transakcija, odnosno njegov integritet, autentičnost i ispravost potvrđuje jedan ili više „validatora“. Za provjeru ispravnosti bloka transakcija „validator“ koristi procesorsku snagu kako bi rješio određeni kriptografski problem (u slučaju Bitcoina koristi se SHA 256 kriptografska funkcija) te je za svako ispravno potvrđivanje bloka transakcija nagrađen određenom količinom Bitcoina koji nastaju automatskim inflacijskim postupkom odnosno „printanjem“ nove količine Bitcoina. Ovaj postupak rješavanja kriptografskog problema odnosno validacijski model se naziva „Proof of work“ (PoW) te je uveden kako bi se zahtjevom za ulaganjem određene količine procesorske snage odnosno rada, spriječilo virtualne (lažne) entitete u sudjelovanju u procesu validacije.

Slika 10: Shematski prikaz procesa validacije transakcije u blockchain mreži



Izvor: Euromoney Learning 2020.

Ispravnost potvrde transakcijskog bloka, odnosno ispravnost postupka validacije koju je proveo nasumično izabrani validator je relativno jednostavno provjeriti te ovaj proces provode ostali „validatori“. Nakon što je među validatorima ustanovljen koncenzus po pitanju ispravnosti validacije (više od 50% validatora se slaže s ishodom) bloka, transakcije tog bloka se konačno provode te se blok dodaje u digitalni zapis odnosno knjigu transakcija (eng. ledger), čija je kopija spremljena na svakom „validatoru“. Nakon svakog potvrđenog bloka transakcija knjiga transakcija se ažurira dodajući novi blok na lanac koji tvore prethodni blokovi. Iz ovog postupka je i nastao sam naziv „Blockchain“ odnosno izravno prevedeno – „lanac blokova“.

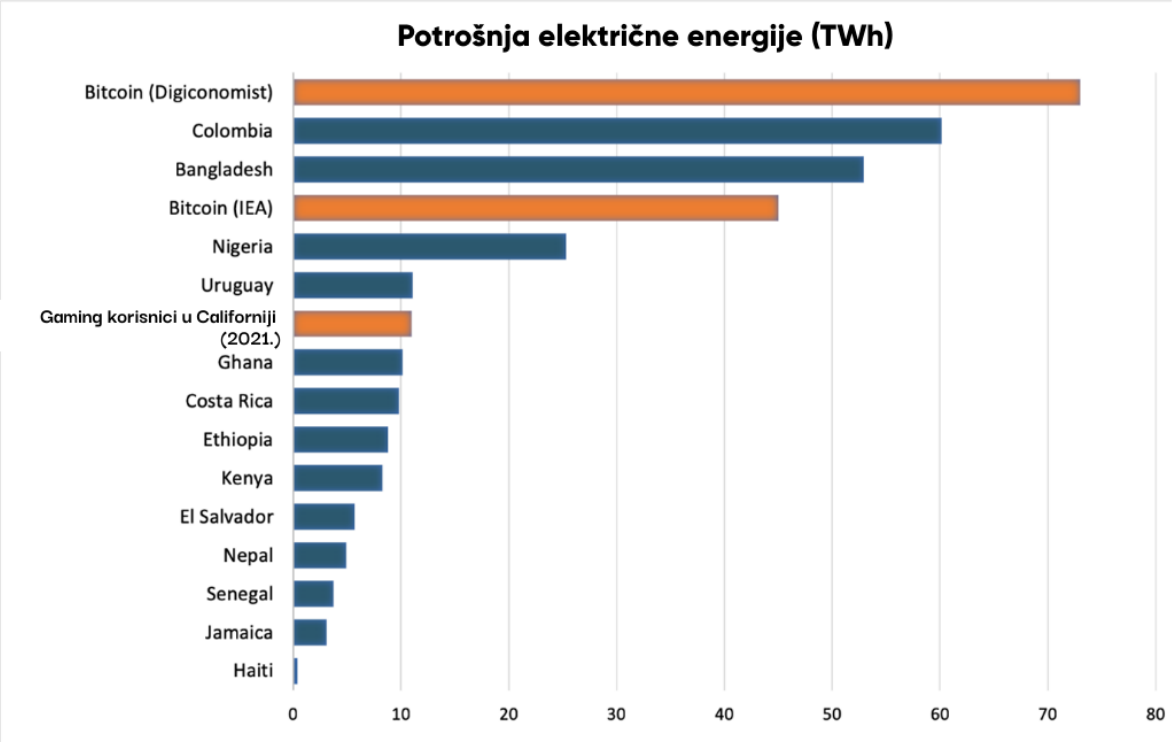
3.2 Osiguravanje mreže – rudarenje

Iz prethodnog poglavlja možemo zaključiti kako je sigurnost Bitcoin mreže bazirana na pretpostavci kako „pošteni“ validatori (rudari) kontroliraju većinu procesorske snage odnosno računalnih resursa te da je glavni motivacijski čimbenik za sudjelovanje u validacijskom procesu nagrada koja se automatski distribuira po ispravno obavljenoj validaciji. S obzirom da je Bitcoin sustav distribuiran i probabilistički, odabir validatora se odvija nasumično sa šansama proporcionalnim računalnoj snazi koju validator predstavlja u mreži. Stoga se, kako bi ostvarili barem djelomičnu nagradu, validatori sa manjom računalnom snagom grupiraju u takozvane „Mining pool-ove“ čime povećavaju ukupnu računalnu snagu te samim time i vjerojatnost odabira za validaciju određenog bloka. Postoji niz problema i rizika koji mogu

nastati u ovakvom organizacijskom uređenju „validatora“ koji sežu od neisplate nagrade rudarima od strane rukovodioca Mining Pool-a do pokušaja ostvarivanja većinskog udjela u ukupnoj računalnoj mreži čime bi se otvorio put prema potpunoj kontroli transakcijske mreže od strane jednog entiteta.

Također, s obzirom na eksponencijalan rast broja transakcija na Bitcoin mreži u posljednjih nekoliko godina, jedan od bitnijih problema je postala i potrošnja energije koja je potrebna za rješavanje kriptografskog problema odnosno validaciju transakcija. Količina energije koja je potrebna za osiguravanje ove mreže je prerasla potrošnju ukupne energije u pojedinim državama kao što su Argentina, Kolumbija, Bangladeš te ga CCAF (Cambridge Center for Alternative Finance) procjenjuje na 110 TWh odnosno 0,55% ukupne svjetske potrošnje energije (Slika 11.). Ova tema je detaljnije analizirana u poglavlju sljedećem poglavlju.

Slika 11. Usporedba potrošnje energije bitcoina i određenih država



Izvor: https://www.energyforgrowth.org/ 2019.

3.3 Prednosti blockchain tehnologije u odnosu na tradicionalne transakcijske sustave

U ovom poglavlju su sumirana saznanja iz prethodnog poglavlja koje sadrži tehnički opis blockchain tehnologije te su prezentirane konkretne prednosti i potencijalni rizici u praktičnoj primjeni ove tehnologije (M. Conti i dr, 2017: 7-9) .

1.) Ne postoji centralni element – treća strana:

S obzirom da se validacija i knjiga transakcija u Bitcoin mreži provodi i ažurira putem velikog broja validatora organiziranih u distribuiranu mrežu, nema potrebe za centralnim regulacijskim elementom. Broj validatora može biti beskonačan te je kopija knjige transakcija spremljena na svakom validatoru te ažurirana nakon svakog uspješnog bloka. Ovakva struktura je izrazito robusna i praktički se ne može zaustaviti sve dok postoji barem minimalni broj validatora u mreži. U slučaju prestanka rada određenog broja validatora, osiguravanje mreže preuzimaju drugi validatori tako da je gotovo nemoguće „ugasiti“ mrežu izoliranjem određene skupine servera ili čak cijele države kao što je pokušala Kina. U blockchainu ne postoji centralni autoritet koji bi mogao manipulirati podatcima ili nenamjernom greškom nanijeti štetu korisnicima mreže. U idealnim uvjetima, pri čemu se najviše težišta stavlja na edukaciju korisnika, blockchain je sa tehničke strane gledano izrazito siguran transakcijski sustav.

2.) Anonimnost i transparentnost:

Ove dvije značajke blockchaina se djelomično međusobno isključuju. Određena razina anonimnosti je postignuta zbog korištenja digitalnog novčanika sa adresom za izvršavanje transakcijskih aktivnosti. Umjesto osobnih podataka korisnika koji se predaju centralnom autoritetu i bazi podataka, korisnik u blockchain transakcijskom sustavu je predstavljen putem digitalnog novčanika čija adresa je skup brojki i slova te ne zahtjeva unošenje nikakvih osobnih podataka za korištenje. Nadalje, korisnik može imati i više digitalnih novčanika sa različitim adresama čime se može postići veća razina anonimnosti, pogotovo ukoliko se iz nekog razloga korisnika uspije povezati sa određenim digitalnim novčanikom.

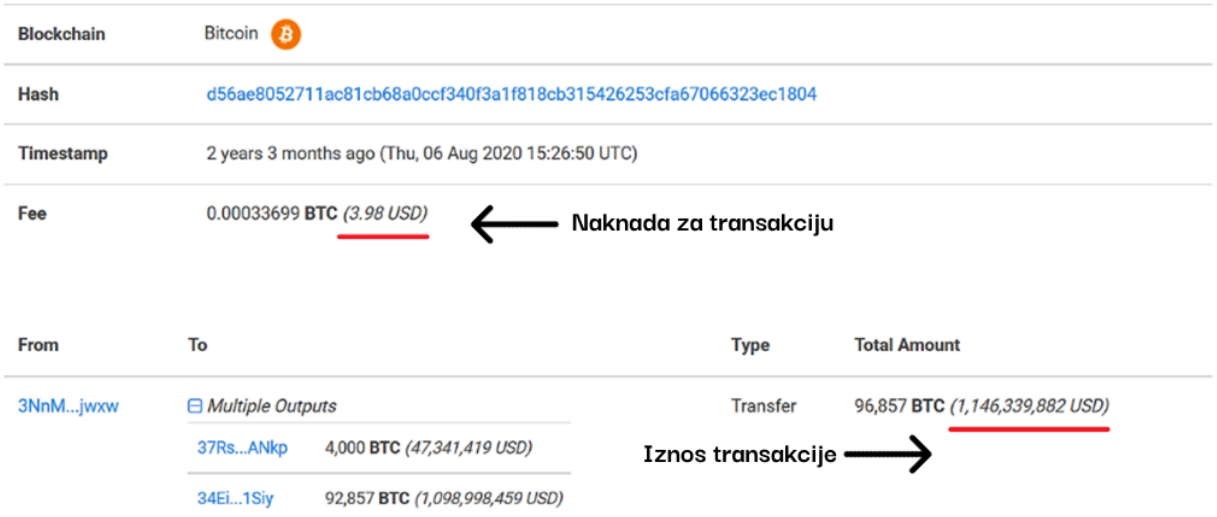
Kako je u blockchain sustavu knjiga transakcijskih zapisa spremljena na svakom validatoru, aktivnosti na mreži su potpuno transparentne te su informacije o transakcijama javno dostupne u svakom trenutku. Ovakva struktura knjige transakcija (knjiga zapisa) pomaže u ranom otkrivanju i prevenciji potencijalnih malicioznih aktivnosti na mreži te je forenziku

određenog štetnog događaja i „post mortem“ izvješća zapravo puno konkretnije provesti na blockchain transakcijskom sustavu. Upravo zbog ove značajke možemo reći da je blockchain zapravo pseudo-anoniman, jer nudi određenu razinu anonimnosti uz maksimalnu transparentnost mrežne aktivnosti. Jednom kad se odredi pravi identitet korisnika koji stoji iza adrese digitalnog novčanika, moguće ga je, bez ikakvih vjerodajnica, povezati sa kompletnom povijesti svih transakcija koje je korisnik obavio sa istim novčanikom. Upravo zato razina anonimnosti koju korisnik može postići na blockchain mreži ovisi primarno o razini zaštite osobnih podataka koju sam korisnik mora provoditi prilikom interakcije sa digitalnim aplikacijama.

3.) Skalabilnost i niske transakcijske naknade:

U poglavlju 1.3 spomenute su novije transakcijske „kripto“ mreže koje uz transparentnost, decentraliziranost i sigurnost nude i izrazito veliki potencijal u pogledu brzine, transakcijske naknade i broja transakcija koje mreža može provesti u određenom vremenskom periodu. Većina ovakvih mreža, kao što je Solana, Cosmos, Algorand, Avalanche i druge još nisu zadobile dovoljan broj korisnika i likvidnosti, te su neke od njih još uvijek u razvoju radi čega ne mogu biti korištene kao pouzdana infrastruktura za globalnu primjenu. S druge strane Ethereum mreža je od 2017. godine pokazala besprijekornu robusnost, ali uz slabije performanse (visoke cijene transakcija i nizak broj transakcija u sekundi) te se u narednom periodu očekuje nadogradnja mreže koja bi omogućila bolje performanse uz zadržavanje maksimalne sigurnosti i pouzdanosti. Vrijednost transakcije u ovakvim mrežama često premašuje 100 milijuna dolara uz zanemarive transakcijske naknade koje ponekad iznose manje od 0.00001% vrijednosti transakcije (Slika 12.).

Slika 12. Prikaz detalja transakcije Bitcoina u vrijednosti od preko milijardu dolara



Izvor: https://whale-alert.io/ 2019.

4.) Pristupačnost i plaćanja:

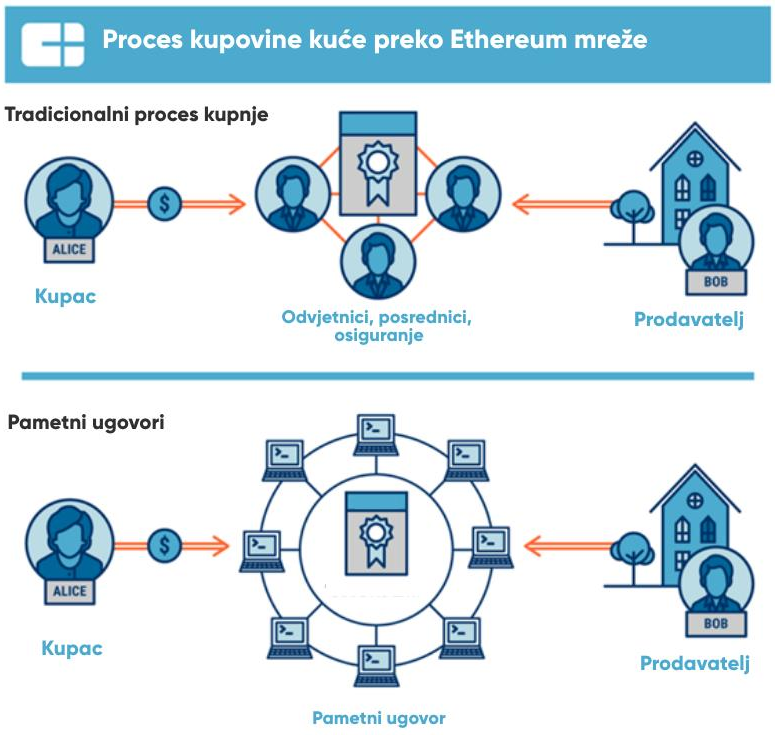
Jedna od najvećih prednosti blockchain transakcijskih sustava u odnosu na tradicionalne bankarske sustave je pristupačnost. Blockchain transakcijske mreže su dostupne 24 sata dnevno, 7 dana u tjednu te se vrijeme finalizacije transakcije kreće od 1 sekunde (Cosmos, Solana) do 10 minuta (Bitcoin, Ethereum) neovisno o geografskoj poziciji pošiljatelja i primatelja određene transakcije. Ovakve značajke su moguće zbog distribuirane arhitekture blockchain sustava te predstavljaju višestruko napredniju tehnologiju i praktičnu primjenu u odnosu na tradicionalne bankarske sustave, posebno u sektoru plaćanja gdje bankarskom sustavu nerijetko treba i nekoliko dana za procesuiranje pojedinih transakcija.

5.) Kreditiranje i likvidacije dugova – pametni ugovori:

Blockchain transakcijski sustavi kao što je Ethereum omogućuju postavljanje takozvanih pametnih ugovora (eng. Smart contract) na mrežu. Pametni ugovor je računalni kod koji uređuje odnos između dvije ili više strana te automatski provodi odredbe ugovora u slučaju zadovoljenja uvjeta određenih stavki tog ugovora. Podaci o pojedinom pametnom ugovoru su pohranjeni na blockchainu te su javno dostupni. Pojava ove tehnologije na blockchainu je započela ekspanziju Ethereum mreže (trenutno druga digitalna valuta po tržišnoj kapitalizaciji)

te razvoj nove vrste financijskog tržišta – Decentralizirane Financije (skraćeno DeFi). Velika popularnost DeFi-ja je uvjetovana naprednijim financijskim proizvodima koji su omogućili jednostavnije kreditiranje, zajmove, likvidacije i trgovanje bez potrebe za centralnim tijelom kao u bankarskom sustavu. Također ukoliko je odnos između npr. zajmodavca i zajmoprimca uređen kvalitetnim pametnim ugovorom, rizik neplaćanja tog zajma je ograničen skoro isključivo na vanjske faktore. Primjer operativne primjene pametnih ugovora je razvoj registra zemljišnih knjiga u Ujedinjenim Arapskim Emiratima čime je transparentnost i pravovaljanost ugovora osigurana digitalno, bez angažiranja trećih strana kao što su odvjetnici, agenti itd. (Slika 13.)

Slika 13. Primjer kupnje nekretnine preko pametnih ugovora



Izvor: https://houseoftrade.ca/blockchain-technology-real-estate/ 2020.

6.) Sigurnost:

Krađu digitalnih valuta je teoretski moguće odraditi jedino ukoliko je privatni ključ digitalnog novčanika poznat kriminalnim akterima. Dizajn Bitcoina pruža iznimno visoku razinu sigurnosti jer je za razliku od tradicionalnih vrsta plaćanja poput kreditnih kartica, privatni ključ skriven tijekom provođenja transakcije. Također, ne postoji način da se transakcija

provedena na blockchain mreži poništi odnosno da se sredstva koja su poslana na pogrešnu adresu vrate pošiljatelju. Ovakav dizajn osigurava izbjegavanje dvostrukih i nepostojećih plaćanja te štiti primatelja Bitcoin digitalnih tokena. Nedostatak ovog dizajna je što, ukoliko je korisnik omaškom unio krivu adresu primatelja te potvrdio transakciju, nije moguće vratiti poslana sredstva na adresu pošiljatelja odnosno reverzirati transakciju.

7.) Dionice, obveznice i druga tržišta kapitala:

Tokenizacijom dionica, obveznica i drugih vrijednosnih papira, Blockchain tehnologija omogućuje efikasnija, interoperabilna tržišta. Iako je ovaj sektor u Blockchain sustavima još uvijek u ranoj fazi, sve veći broj tradicionalnih financijskih vrijednosnica osigurava likvidnost na nekoj od Blockchain mreža, čineći svoje vrijednosnice dostupnima širokom spektru populacije koje u pravilu ne koriste ili zaziru od tradicionalnih investicijskih proizvoda. Također, vođenje knjige zapisa i trgovanja je puno jednostavnije putem ove tehnologije, operativni troškovi su minimalizirani, a transparentnost je na najvišem nivou.

3.4 Nedostatci blockchain tehnologije u odnosu na tradicionalne transakcijske sustave

1.) Velika potrošnja energije:

Bitcoinov model distribuiranog koncenzusa kojim se validiraju transakcije u mreži (PoW) čini ovu Blockchain tehnologiju izrazito otpornom na sigurnosne prijetnje, ali u isto vrijeme troši ogromnu količinu energije i računalnih resursa u odnosu na tradicionalne transakcijske sustave. Jedna transakcija putem Bitcoin mreže troši do 5000 puta više energije od VISA transakcije (M. Conti i dr, 2017: 8).

Ipak, novije generacije blockchain mreža stavljaju ekološku komponentu visoko na ljestvici poželjnih osobina, jednim dijelom i zbog regulativnih restrikcija vezanih uz potrošnju energije koje su najavljene od strane pojedinih država.

Pozitivni primjer razvijene ekološke svijesti u blockchain tehnologijama je nedavno poboljšanje Ethereum mreže, koja je promjenom modela distribuiranog koncenzusa (sa PoW na PoS) smanjila potrošnju energije potrebne za osiguravanje mreže za 99.99% odnosno sa 23 milijuna MWh na 2600 MWh godišnje (Decrypt, 2022).

2.) Gubitak kontrole nad digitalnim novčanikom:

S obzirom da u Blockchain transakcijskim sustavima ne postoji centralni autoritet koji bi „skladištio“ i imao pristup svih sigurnosnim ključevima svakog korisnika mreže, gubitak ili kompromitacija sigurnosnog ključa dovodi do nepovratnog gubitka svih digitalnih sredstava na zahvaćenom digitalnom novčaniku. Najčešći slučajevi su: gubitak uređaja koji čuva sigurnosni ključ (takozvani hard wallet), kompromitacija novčanika instaliranog na računalu (hakiranje, phishing itd.) te kvar jedinog uređaja na kojem je pohranjen sigurnosni ključ. Ukoliko korisnik izgubi sigurnosni ključ digitalnog novčanika, radi specifične sigurnosne arhitekture digitalnih novčanika ne postoji način za „spašavanje“ digitalnih sredstava s istog. Analiza tvrtke za digitalnu forenziku Chainanalysis iz 2017. godine pretpostavlja da je između 2.78 i 3.79 milijuna Bitcoina pohranjeno na digitalnim novčanicima nad kojima su vlasnici izgubili kontrolu. Ova količina odgovara između 15 i 20% ukupne cirkulacijske količine Bitcoina odnosno između 55 i 76 milijarde dolara trenutne vrijednosti (Listopad 2022.).

3.) Kriminalna aktivnost:

Visok stupanj anonimnosti koju pružaju blockchain transakcijski sustavi omogućavaju i olakšavaju izvršavanje raznih kriminalnih aktivnosti kao što su iznude, izbjegavanje poreza i porezne prevare, plaćanja na crnim tržištima i pranje novca. Sigurnosne strukture se puno sporije prilagođavaju tehnološkom napretku te u pravilu kasne sa prilagodbom zakonskih i regulativnih okvira te samom operacionalizacijom istih.

4. NOVI SIGURNOSNI IZAZOVI KOJE JE UVJETOVALA POJAVA DIGITALNIH VALUTA

Digitalne valute su tehnička i financijska inovacija koja predstavlja veliki potencijal za globalnu ekonomiju. Radi određenih tehničkih prednosti pri operacijama transakcije vrijednosti te slabe regulacije i nadzora ovog prostora, ova tehnologija se često koristi za kriminalne svrhe. Korištenje digitalnih valuta za kriminalne aktivnosti i pranje novca je poraslo tijekom proteklih godina u smislu obujma i sofisticiranosti. Kao posljedica, kriminalna uporaba digitalnih valuta više nije ograničena na aktivnosti kibernetičkog kriminala, već se sada odnosi na sve vrste kriminala koji zahtijevaju transakciju vrijednosti odnosno novca. Privatni sektor, odnosno mjenjačnice digitalnih valuta, izvješćuju da korištenje digitalnih valuta u ilegalne svrhe čini mali dio njihove ukupne upotrebe, odnosno 0,34% svih transakcija. Nasuprot tome, istraživanja akademske zajednice procjenjuju mnogo veći promet u kriminalne svrhe pa su povezali čak 23% transakcija digitalnih valuta sa kriminalnim aktivnostima. (Europol: 2022)

Kako bi klasificirali nove rizike i prijetnje nacionalnoj sigurnosti koje su proizašle iz pojave i tehnološkog napretka blockchain tehnologije , možemo se poslužiti Direktivom Vijeća EU 2016/1148, koja govori o implementaciji mjera za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije. Kako se navodi u objavi Ureda Vijeća za nacionalnu sigurnost RH - „Implementacijom Direktive uspostavit će se veća sigurnost ključnih usluga u definiranim sektorima (energetika, transport, bankarstvo, infrastrukture financijskog tržišta, zdravstveni sektor, opskrba i distribucija vode, digitalna infrastruktura) te kaskadno svih drugih procesa koji se oslanjaju na takve usluge. Direktiva donosi i preporuke za pružatelje digitalnih usluga (Internetsko tržište, Internetske tražilice, usluge računalstva u oblaku) koje je potrebno uskladiti u okviru država članica.“

Ova direktiva opisuje digitalne valute kao „infrastrukturu unutar infrastrukture, te je označava kao potencijalnu ugrozu nacionalnoj sigurnosti radi omogućavanja kršenja zakona te nanošenja materijalne štete putem digitalnih platformi. Direktiva klasificira sljedeće kategorije ugroza koje su uvjetovane razvojem digitalnih valuta:

1. Digitalne valute kao infrastruktura za kriminalnu aktivnost
    a. Sredstvo kriminalne aktivnosti
        i. Internetska platforma za trgovinu drogom

ii. Ilegalna trgovina u širem smislu (Darknet)
iii. Izbjegavanje poreza
iv. Pranje novca
v. „Layering“ novca
vi. Tranzit novca

b. Objekt kriminalne aktivnosti
i. Krađa
ii. Prevara
iii. Korupcija

2. Prijetnje ekonomskoj sigurnosti
a. Direktni oblici
i. Ilegalna trgovina
ii. Izbjegavanje poreza
iii. Ilegalne financijske-bankarske aktivnosti
iv. Pranje novca
v. Porezne prevare
vi. Tranzit novca
vii. Korupcija

b. Indirektni oblici
i. Konkurentnost
ii. Socijalna neubrojivost
iii. Ne transparentno lobiranje
iv. Povjerenje u institucije

3. Prijetnje općoj sigurnosti
a. Direktni oblici
i. Organizirani kriminal
ii. Trgovina drogom
iii. Kriminalne aktivnosti
iv. Prevare
v. Porezne prevare i izbjegavanje poreza

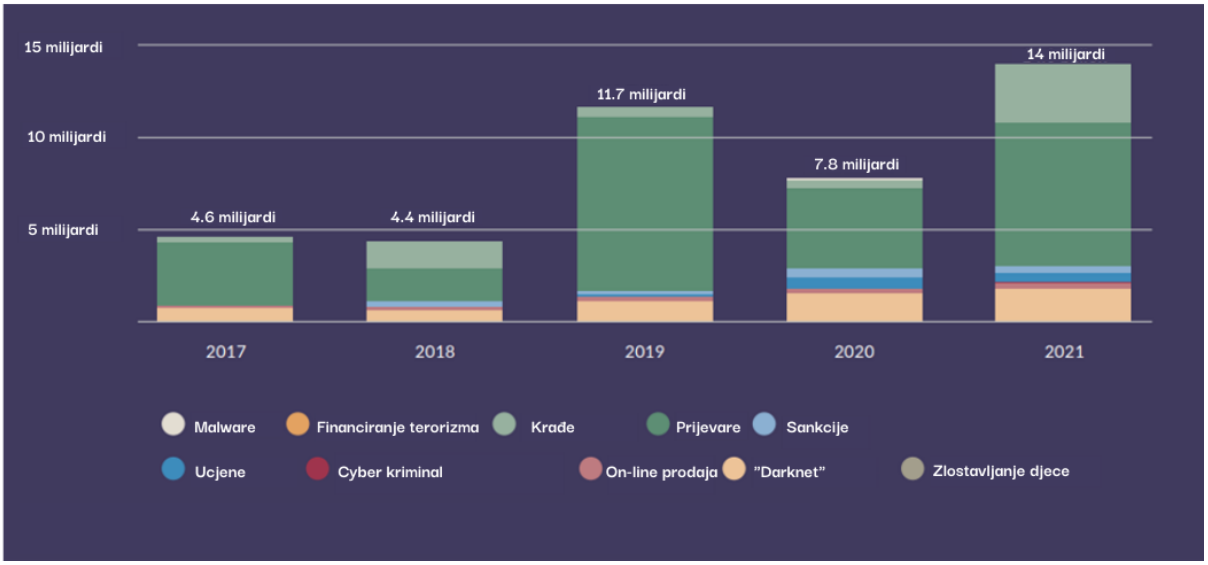
b. Indirektni oblici
i. Financiranje terorizma
ii. Hibridne ugroze (kibernetičke i informacijske prijetnje; financiranje interesnih skupina)

iii. Ugroze objektima kritične infrastrukture

4.1 Nezakoniti tranzit novca putem digitalnih valuta

Samo u 2021. ukupni promet digitalnim valutama porastao je za 567 posto - u usporedbi sa razinom iz 2020. na 15,8 trilijuna USD (Coingecko 2022.). S obzirom na taj brzi rast, udio potvrđenih nezakonitih aktivnosti provedenih putem digitalnih valuta ipak nije pratio taj rast te je porastao za „samo“ 79 %. Ista analiza tvrtke Chainanalysis je potvrdila porast u prometu nezakonitih aktivnosti sa 7,8 milijardi USD u 2020. na 14 milijardi u 2021. Štoviše, ove procjene mogu podcijeniti udio nezakonitih aktivnosti kroz nedostatke u obavještajnim podacima, koji previđaju nedopuštene aktivnosti izvan mreže (eng. Off-chain) koje uključuju prijevaru, pranje novca i druge prikrivene aktivnosti.

Slika 14. Potvrđeni promet ilegalnih aktivnosti putem digitalnih valuta



Izvor: Chainanalysis 2021.

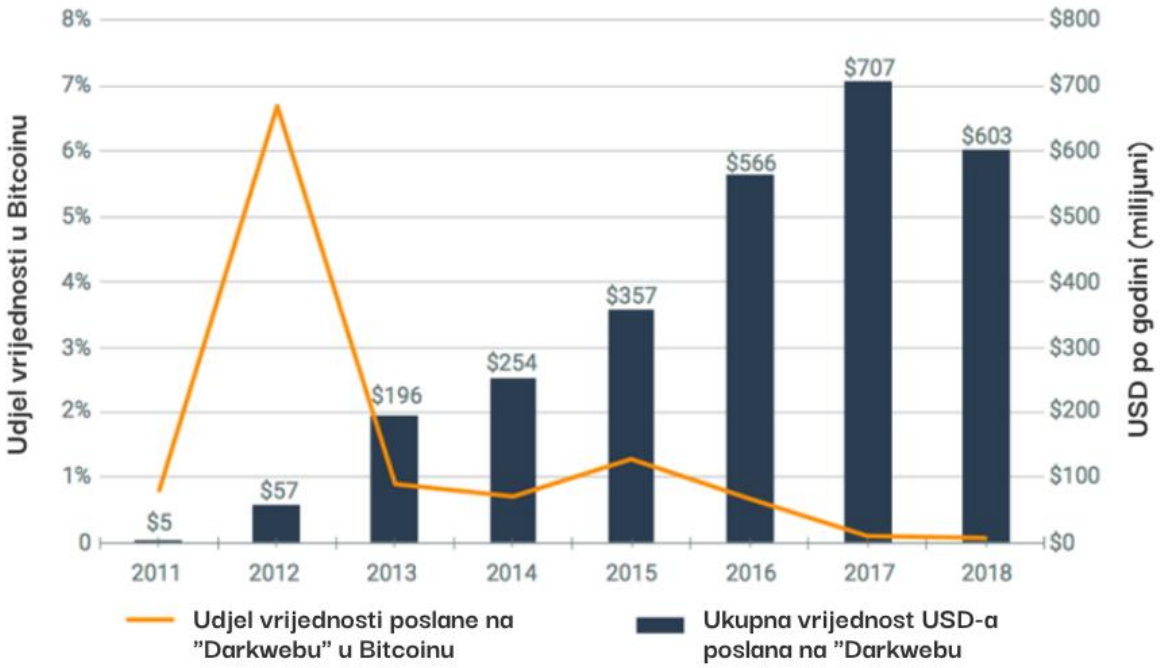
S druge strane, Chainanalisisova analiza iz 2021., pokazuje da su u 2020. nezakoniti subjekti primili oko 5 milijardi dolara sredstava (Slika 14.), te su nezakoniti subjekti poslali oko 5 milijardi dolara drugim subjektima, što predstavlja manje od 1% ukupnih tokova digitalnih valuta. Ovaj omjer, zakonitog i nezakonitog prometa digitalnih valuta je u periodu između 2011. i 2019. godine iznosio između 60 i 80% (Eliptic). Znakovit pad u prometu digitalnim valutama među nezakonitim subjektima, unatoč izrazitom porastu apsolutnog prometa digitalnim valutama u zadnjih par godina, rezultat je regulativnih pritisaka vlada koje su prisilile mjenjačnice digitalnih valuta na primjenu strožih AML (eng. Anti Money

Laundering) i KYC(eng. Know-Your-Customere) propisa. Kriminalne aktivnosti tako su se preselile na neregulirane mjenjačnice koje su izvan jurisdikcija te samim time nemaju stroge regulativne zahtjeve. Krajnji rezultat su veći troškovi pranja i „layeringa“ novca zbog lošije likvidnosti ovakvih mjenjačnica.

4.2 Digitalne valute kao infrastruktura za ilegalne aktivnosti i trgovinu

Povezanost kriptovaluta s ilegalnim tržištem prvi put je privukla pozornost 2013. nakon zabrane rada i uhićenja osnivača Silk Road-a 2013., - web stranice specijalizirane za trgovanje ilegalnim proizvodima i uslugama, a kojoj se može pristupiti samo putem Dark Weba. Silk Road je 2011. nastao kao internetska trgovina (eng.marketplace) koja je povezivala ilegalne prodavače droge sa zainteresiranim kupcima, uz potpunu zaštitu njihovih identiteta i transakcija. Stranica je bila dostupna samo putem mreže poznate kao Tor, koja postoji uglavnom za anonimiziranje korisničkih podataka i online aktivnosti odnosno skrivanje IP adrese korisnika. Kao sredstvo i medij naplate navedenih ilegalnih proizvoda, korištena je digitalna valuta Bitocoin, čime se osiguravao dodatni stupanj anonimnosti i „zaštite“ korisnika ove platforme. S obzirom da je knjiga transackcija na Bitcoin mreži otvorenog tipa, svatko je mogao pristupiti podacima o transakcijama u realnom vremenu. Unatoč stupnju anonimnosti koji je pružalo korištenje Bitcoin adrese umjesto imena i prezimena, transparentnost knjige transakcija (eng.ledger) je potaknula razvoj dodatnih sredstava anonimizacije transakcijskog procesa pa se u narednim godinama pojavljuju „dark wallets“ i „Privacy Altcoins“ kao što je Monero, koji pružaju još veću razinu anonimnosti. FBI i DEA su ipak uspjeli ugasiti Silk Road platformu pri čemu su zaplijenili više od 144,000 Bitcoina (tadašnja vrijednost 34 milijuna dolara) te uhitili osnivača Rossa Ulbrichta koji je po procjenama FBI-a zaradio više od 80 milijuna dolara od provizija na trgovinu putem Silk Roada (Investopedia: 2021.).

Slika 15: Usporedba ekonomske vrijednosti Bitcoina i dolara poslanog na DarkWeb u periodu 2011.-2018.

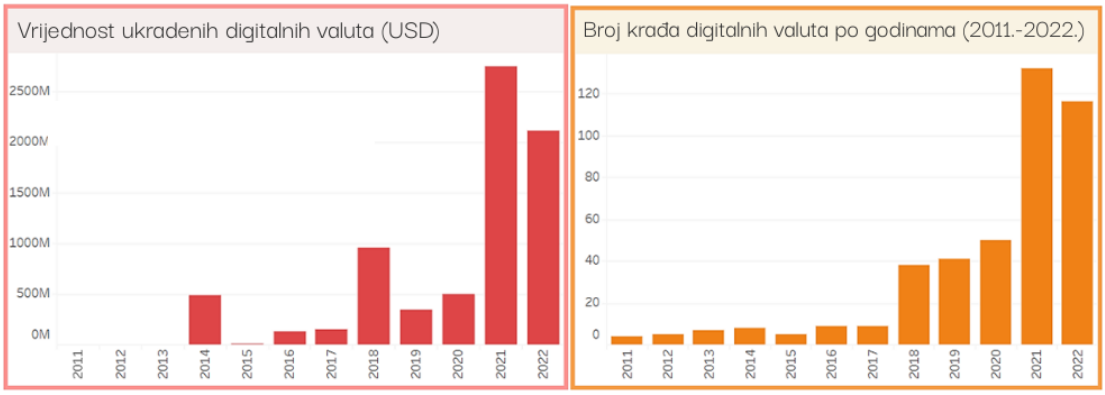


Izvor: Chainanalysis (2019.)

4.3 Digitalne valute kao platforma za kriminalne radnje krađe i prevare

U 2019. godini Forbes je objavio da su 2019. hakeri ukrali 1,7 milijardi USD u digitalnim valutama dok je 950 milijuna USD ukradeno iz mjenjačnica i infrastrukture digitalnih valuta, što je 3,6 puta više nego 2017. U 2020. godini Chainanalysis je procijenio porast krađa digitalnih valuta od 516%, na ukupnu brojku od 3,2 milijarde dolara od čega je više od 70% vrijednosti ukrano iz DeFI-ja. Porast prometa u DeFi-ju od 912% te porast broja korisnika blockchaina na gotovo 100 milijuna, u kombinaciji sa lošom sigurnosnom kulturom pri korištenju digitalnih decentraliziranih aplikacija, rezultirao je poražavajućim brojkama za prostor decentraliziranih financija. Nedostatak regulativnog okvira te visok stupanj anonimnosti ohrabrili su kriminalce u provođenju kaznenih djela krađe i prevare te su u istima postali iznimno kreativni.

Slika 16: Broj i vrijednost krađa digitalnih valuta u periodu 2011.-2022.



Izvor: https://www.comparitech.com/crypto/biggest-cryptocurrency-heists/

Najčešća vrsta krađa u DeFI-ju su vezane uz krađu ili iznuđivanje sigurnosne fraze digitalnog novčanika korisnika kojem se kriminalci predstavljaju kao tehnička podrška, koja je u DeFI projektima izrazita rijetkost, ili slanjem linkova koji vode na kompromitirane web aplikacije koje izgledom podsjećaju na originalne. Čim korisnik pristupi takvim aplikacijama te potvrdi „spajanje“ na iste, kriminalci dobivaju potpuni pristup njegovom digitalnom novčaniku s kojeg potom prebace sva digitalna sredstva na vlastiti novčanik. U ovakvim prevarama koriste se i „phishingom“ kao već standardnom metodom obmanjivanja korisnika raznih financijskih aplikacija i ostalih aplikacija koje koriste osobne podatke korisnika.

Relativno nova vrsta prevare je takozvani „rug pull“ („povlačenje tepiha“), u kojem se korisnicima decentraliziranih mjenjačnica predstavlja projekt koji nema osiguranu likvidnost, odnosno većina likvidnosti, koja se nalazi na decentraliziranoj mjenjačnici, je u vlasništvu vlasnika kriminalnog projekta. Nakon što digitalna valuta dosegne određenu cijenu, vlasnik likvidnosti povlači likvidnost sa mjenjačnice te je prodaje za neku drugu valutu, nakon čega korisnici i vlasnici digitalnih tokena ostaju sa digitalnim tokenima koji su bezvrijedni.

Slika 17. Najveće krađe u povijesti digitalnih valuta

Izvor: Statista 2022.

Točan podatak o broju i vrijednosti ukradenih digitalnih valuta skoro je nemoguće točno odrediti no možemo promotriti najveće krađe koje su se dogodile u vrlo kratkom periodu od pojave digitalnih valuta do danas. Ako bi usporedili krađu digitalnih valuta s krađom fizičkog novca došli bi do zanimljivog podatka; najveće poznate krađe banaka bile su 920 milijuna USD u Bagdadu 2003. (tijekom ratnog razdoblja), 282 milijuna USD u Bagdadu 2007. i 97 milijuna USD u Londonu 1987. (MoneyWise, 2018.) (Statista, 2022). Najveće krađe digitalnih valuta su PolyNetwork (2021.) 611 milijuna USD, Ronin (2022.) 540 milijuna USD, Coinheck (2018.) 534 milijuna USD, Mt.Gox (2014.) 480 milijuna USD (Statista 2022.). Iz navedenog možemo izvesti 3 zaključka: velike krađe digitalnih valuta se događaju češće nego velike krađe fizičkog novca, vrijednosti krađa su nerijetko preko 400 milijuna USD, velike krađe digitalnih valuta su u porastu te su dosegle vrhunac tijekom „bull run-a“ 2021.-2022. godine.

4.4 Digitalne valute kao platforma za izbjegavanje poreza

Utaja poreza važan je društveno-ekonomski problem u svim društvima svijeta, bez obzira na vrstu poreznog sustava ili stupanj gospodarske razvijenosti zemlje. Digitalni tehnološki razvoj (web 3.0, DeFI) donosi nove fenomene poput digitalne sive ekonomije u centru koje je utaja poreza. Prema Remeikienė et al. (2018) „digitalna siva ekonomija odnosi

se na ilegalne aktivnosti, poput pružanja i prodaje digitalnih usluga roba/usluga na mreži, kada iznimno djeluju u digitalnom prostoru, subjekti krše postojeće pravne norme i propise s težnjom za nezakonitim obostranim interesom i materijalnim pogodnostima". Anonimnost, brzina transakcija te izostanak kontrole i nadzora nad transakcijskim procesom čine digitalne valute gotovo savršenim sredstvom za izbjegavanje poreza.

Mreže specijalizirane za pranje novca velikih razmjera su usvojili digitalne valute i nude svoje usluge drugim kriminalnim akterima. Korištenje digitalnih valuta u shemama pranja novca je u porastu, a mnoge su se kriminalne mreže oslanjale na digitalne valute kao sredstvo plaćanja tijekom pandemije COVID-19 (Europol spotlight, 2019.). Te se mreže mogu osloniti na već uspostavljene infrastrukture kao što su brojni bankovni računi kao i dubinsko znanje bankovnog sustava i korištenje FinTech-a. Mreže za pranje novca pružaju svoje usluge drugim kriminalnim mrežama, koje mogu uključivati stjecanje ili trgovinu digitalnim valutama, legalizaciju imovine stečene kriminalom i konačnog unovčavanja na računima kriminalaca. Profesionalne mreže za pranje novca značajna su prijetnja i omogućuju drugim kriminalcima uvjete za rad.

4.5 Digitalne valute kao sredstvo financiranja terorizma

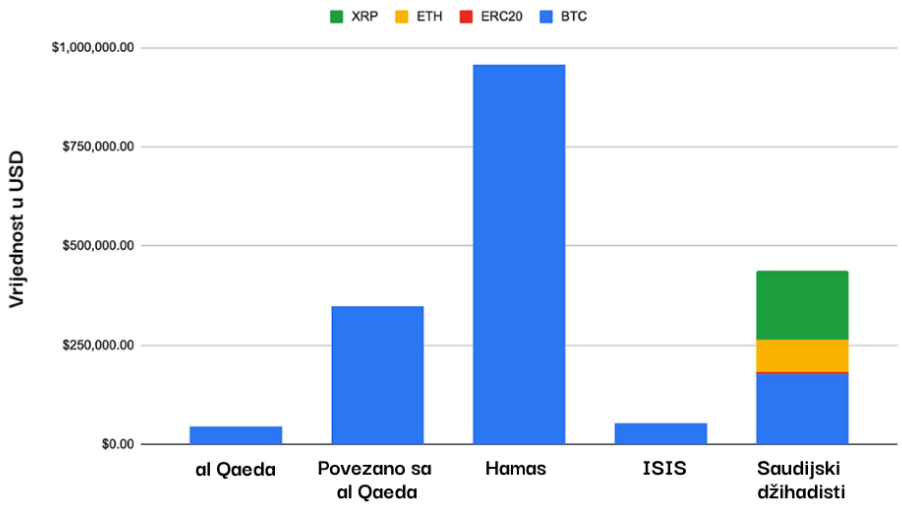
Izazovi koji predstavljaju digitalne valute nisu ograničeni samo na Bitcoin. U posljednjih nekoliko godina pojavile su se mnoge nove digitalne valute, uključujući alternativne valute (eng. altcoins) kao što je Omni Layer (MasterCoin), BlackCoin i Monero, koji se reklamiraju kao digitalni transakcijski sustavi sa većom razinom privatnosti od Bitcoina. Monero, najveća od ovih valuta, sebe predstavlja kao "sigurnu i privatnu mrežu čijim je transakcijama nemoguće ući u trag" te se stoga počeo prihvaćati na internetskom darknetu tržišta za droge. Druge digitalne valute kao što je Hawk, omogućile su potpuno privatne ugovore i transakcije na Ethereum blockchainu. Upravo ovaj prelazak sa pseudo-anonimnosti na potpunu anonimnost bez mogućnosti povezivanja pošiljatelja i primatelja transakcije je ključna znčajka navedenih blockchain mreža i aplikacija, koja ih čini pogodnom za korištenje u svrhe financiranja terorizma.

U svibnju 2022. godine OFAC (Ured za kontrolu strane imovine) je sankcionirao mikser digitalnih valuta Blender nakon velikog hakiranja projekta Axie Infinity od 620 milijuna dolara gdje su hakeri koristili upravo ovaj mikser kako bi prikrili transakcije ukradenih digitalnih tokena (Forbes, 2022.). Ovo je bio početak sankcioniranja miksera digitalnih valuta

od strane OFAC-a prije nego što je u kolovozu 2022. godine sankcioniran programer Tornado Cash- a zbog navodnog pranja 7 milijardi dolara od 2019. što je izazvalo osuđivanje od strane kripto zajednice s obzirom da je Tornado Cash „open-source“ platforma te se ova intervencija OFAC-a okarakterizirala kao čin koji cilja na slobodu digitalnog izražavanja. Mnogi članovi kripto zajednice su osudili ovakav čin usmjeren na proizvođača digitalnog proizvoda te koristili analogiju s proizvođačima oružja, čiji se proizvodi mogu koristiti u legalne, ali i u kriminalne svrhe. Tornado Cash čini transakcije na Ethereum, mreži koje su obično javne, nemogućima za praćenje, prikrivajući tragove miješanjem mnogih transakcija zajedno.

Prekidanje protoka novca je ključni element u prekidanju opskrbnih lanaca. Američki predsjednik Trump (2017.) je istakao važnost digitalizacije terorističkih organizacija, te je zaključio da je financijski „supply chain“ prioritet za američku nacionalnu sigurnost odredivši „prekidanje financijskog, materijalnog i opskrbnog lanca ljudstva terorističkih organizacija“ kao jedan od glavnih ciljeva.

Slika 18. Zastupljenost pojedinih digitalnih valuta u financiranju određenih terorističkih organizacija



Izvor: https://www.coinbase.com/ (2021.)

Usporedbom nekoliko terorističkih napada možemo zaključiti da je potrebno relativno skromno financiranje za izvršavanje izrazito „efikasnih“ napada. Za organizaciju napada eksplozivnim napravama u Madridu 2004. godine koji je rezultirao sa 193 žrtve, Al Qaeda je utrošila 100,000 dolara (Gomez,2010). Svjetski Ekonomski Forum (2017.) procjenjuje da je napad auto bombom u Londonu 2007. godine organiziran uz samo 14 000 dolara dok je

teroristički napad kamionom u Nici 2016. godine organiziran sa smiješnih 500 dolara rezultirajući sa 87 žrtava (Limba i dr, 2020: 52-53). Norveški Institut za proučavanje obrane (2015.) navodi da je 68% terorističkih napada organizirano sa budžetom manjim od 10 000 dolara dok je 18% napada izvedeno uz budžet koji nije prelazio 1000 dolara.

Svetlana Martynova, viša pravna službenica u Izvršnoj direkciji Odbora za borbu protiv terorizma Ujedinjenih naroda, izjavila je da se u zadnjih nekoliko godina samo 5% terorističkih napada smatralo financiranima kripto ili povezanima s digitalnom imovinom dok je 2022. godine ta brojka narasla na čak 20% (Reuters, 2022.). Određene mjenjačnice digitalnih valuta, kao što je Coinbase, procjenjuju da je samo 0.05% prometa digitalnim valutama povezano s financiranjem terorizma. Iz svega navedenog možemo zaključiti da je točnu brojku izrazito teško definirati unatoč sve naprednijim alatima za analizu mrežnog prometa digitalnim valutama, ali i da, ukoliko u obzir uzmemo najnižu brojku (Coinbase, 0.05%), je i ta količina novca dovoljna za financiranje velikog broja terorističkih aktivnosti. Regulativa i zakonska tijela su stoga u stalnom razvoju kako bi uspjeli prevenirati i minimalizirati količinu novca koja se putem digitalnih transakcijskih mreža transferira za potrebe terorističkih organizacija.

5. PRILAGODBA SIGURNOSNIH SUSTAVA POJEDINIH DRŽAVA

U prethodnom poglavlju obradili smo specifične tehničke karakteristike digitalnih transakcijskih mreža te rizike koje korištenje takvih mreža predstavlja za državnu, osobnu i društvenu sigurnost. Određene države su stoga odlučile regulirati, a neke potpuno zabraniti korištenje i promet digitalnim valutama. U narednim poglavljima opisani su primjeri zabrane i primjeri regulacije korištenja digitalnih valuta, te primjena regulativa i sigurnosne politike prema digitalnim valutama. S obzirom da su digitalne valute relativno novo tehnološko postignuće, sigurnosne sustave većine zemalja koje ćemo promatrati, možemo reducirati na regulativni odnosno zakonodavni okvir te regulativna financijska tijela koja operacionaliziraju navedene zakonske okvire. Podaci o strategijama i infrastrukturi za nadzor koja se koristi u operativnim tijelima nisu dostupni, a vrlo vjerojatno ni razvijeni u većini zemalja osim u SAD-u, pa i sama analiza tih postupaka i infrastrukture nije izvediva.

5.1. Zabrana digitalnih valuta – Primjer Kine

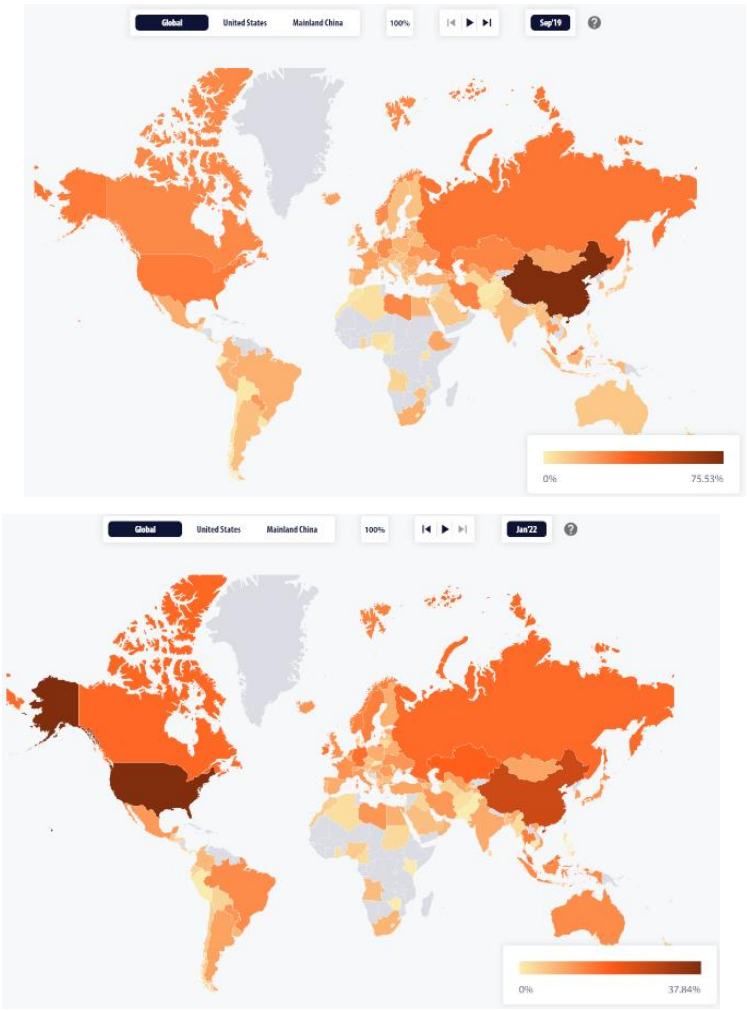
Glavni razlozi radi kojih su određene države zabranile digitalne valute su sljedeći (Frebowitz, 2018: 56-57):

- korištenje digitalnih valuta kao sredstva plaćanja unutar kriminalnih mreža
- slabljenje sposobnosti države da kontrolira tok kretanja kapitala, u zemlji i inozemstvu, u decentraliziranim transakcijskim mrežama
- ograničavanje mogućnosti okupljanja građana protiv države i smanjenje građanskih prava
- eliminiranje konkurentske virtualne valute u pripremi za izdavanje vlastite državne digitalne valute
- eliminiranje velike potrošnje energije uzrokovane validacijom na transakcijskim mrežama

Od svih zemalja koje su pokušale zabraniti korištenje i promet digitalnim valutama, najopsežniji regulativni okvir, a samim time i najbolje rezultate je izvela Narodna Republika Kina. Već od 2013. godine, kada je tržišna kapitalizacija Bitcoina prvi put dosegla značajnu vrijednost (> 1 milijarde dolara) Narodna Banka Kine počela je uvoditi određena regulativna pravila koja su za cilj imala otežavanje u korištenju digitalnih valuta te posljedično smanjenje broja korisnika i samog kapitala koji bi se transferirao digitalnim transakcijskim mrežama. Od početka 2013. godine bankama je zabranjeno vršenje transakcija u Bitcoin tokenima, a do

prosinca 2013. NBK je izdala preporuku o zabrani svih plaćanja povezanih s Bitcoinom svim komercijalnim bankama. Nadalje, monetarna politika NBK je izdala uputu investicijskim bankama te osiguravateljskim kućama sa sličnim smjernicama po pitanju korištenja Bitcoina. U 2014. godini Kina se odlučuje na konkretniji korak te zabranjuje korištenje računa za trgovanje Bitcoin tokenima. Ovakvu vrstu zabrane je moguće operativno primijeniti jedino na centraliziranim mjenjačnicama i/ili fizičkim oduzimanjem uređaja s kojih se primjenjuje digitalna trgovina stoga su kineski korisnici još uvijek mogli izbjeći ovu zabranu te posjedovati Bitcoin na vlastitom digitalnom novčaniku. Kineska vlada 2017. godine se obračunava i sa takozvanim kripto „fundraisingom“ odnosno „Initial Coin Offerings“ (ICO), metodom inicijalnog skupljanja kapitala za projekt koji će se tek u budućnosti realizirati te postaviti na tržište.

Slika 19. Količina računalnih resursa koji sudjeluju u „rudarenju“ po pojedinim državama – usporedba stanja u 2019. i 2021. godini



Izvor: Chainanalysis 2022.

Kina je za potrebe primjene navedenih regulativa koristila i restrikciju pristupa određenim internetskim stranicama te je 2018. godine situacija je eskalirala uvođenjem zakonskih odredbi o restrikciji potrošnje električne energije za potrebe „rudarenja“ digitalnih valuta. Daljnje stezanje obruča oko „rudara“ digitalnih tokena je događa 2019. godine kada je kineska Komisija za Nacionalni razvoj i reforme predložila uvrštavanje „rudarenja“ na listu nepoželjnih industrijskih djelatnosti. S obzirom na količinu računalnih resursa koje su kineski „rudari“ predstavljali u ukupnoj energetskoj bilanci Bitcoin mreže (>50%) te činjenicu da je Kina jedan od vodećih proizvođača procesora koji se koriste za rudarenje, ovakav potez Komisije je izazvao paniku ne samo u Kini već i u ostatku Svijeta.

Konačnu zabranu rudarenja te transakcija i marketinške promocije digitalnih valuta Kina uvodi u 2021. godini te se većina računalnih resursa koji su sudjelovali u validaciji Bitcoin transakcija povlači iz Kine prema SAD-u. Unatoč panici koja je zavladala na tržištu, ovaj transfer „rudara“ je izvršen u iznimno kratkom roku te je SAD preuzeo ulogu glavnog „validatora“ Bitcoin transakcija u Svijetu.

Do 2018. godine još je 5 država uvelo potpunu zabranu korištenja Bitcoina: Bangladeš, Bolivia, Ekvador, Kirgistan i Nigerija. Zakonski propisi u ovim zemljama su izrazito slični te izričito zabranjuju izdavanje, promociju i protok digitalnih valuta, kao i bilo koju digitalnu valutu koja nije izdana od strane centralne banke navedenih država te propisuju kazne zatvora do 12 godina (Bangladeš).

Primjer države koja je uvela djelomičnu zabranu korištenja Bitcoina je Island. Islandska vlada je 2013. godine uvela Zakon o stranim mjenjačnicama kojim je zabranjeno trgovanje digitalnim valutama, ali je posjedovanje i rudarenje digitalnih valuta dozvoljeno. Unatoč ovoj zabrani, Island ostaje atraktivna lokacija u svijetu digitalnih valuta poglavito radi velikih izvora geotermalne energije koja se može koristiti za rudarenje digitalnih valuta.

5.2. Regulacija digitalnih valuta

Kao i navedene države koje su uvele potpunu zabranu digitalnih valuta, razvijene države Svijeta su uvidjele potencijalne rizike koji nastaju popularizacijom digitalnih valuta. Nekoliko faktora je utjecalo na opredjeljenje ovih država prema regulaciji tržišta digitalnih valuta nasuprot potpunoj zabrani. Prvi razlog je jednostavna nemogućnost donošenja zakona koji bi omogućili korištenje cenzure javnog prostora, posebice internetskih stranica, radi demokratskog prozapadnog političkog uređenja ovih država. Također, pojam privatnog

vlasništva je temelj na kojem ove države počivaju stoga bi fizičko oduzimanje računala ili opreme na kojima se nalaze digitalni novčanici prouzrokovalo val negodovanja i osuda javnosti. Drugi razlog opredjeljenja prema regulaciji tržišta je stabilnost ekonomija ovih država. Možemo primjetiti da ekonomije i službene valute država koje su uvele potpunu zabranu digitalnih valuta nisu dovoljno stabilne kako bi izdržale potencijalni odljev kapitala. Potpunom zabranom, države sa visokom stopom inflacije su spriječile tranziciju kapitala u konkurentske valute, kao što je digitalni dolar, posredništvom digitalnih transakcijskih mreža. Potvrda ove politike je i limit koji je Kina uvela na iznošenje tradicionalnih valuta od 50 tisuća dolara godišnje. Napredne zemlje ipak nemaju ovakvih problema te im potencijalni odljev kapitala iz srednje i niže razvijenih država pogoduje, stoga su u reguliranom i kontroliranom tržištu digitalnih valuta pronašle ne samo evoluciju tehnološkom i tržišnom smislu već i alat za osnaživanje vlastite ekonomije.

Glavni razlozi za regulaciju digitalnih valuta (Frebowitz, 2018: 58-59):

- Zaštita potrošača
- Sprječavanje pranja novca
- Zaštita monetarne politike

Države koje su uvele regulaciju suočavaju se sa izazovom pronalaženja adekvatnog stupnja regulacije tržišta koja minimalno zadire u prava građana na posjedovanje digitalnih valuta. Nadalje, definicija digitalnih valuta je širok pojam te je teško izraditi klasifikacijski sustav koji bi pravilo definirao što je digitalna valuta, a što ne. Tehnički modeli digitalnih transakcijskih sustava, koji su zasnovani na distribuiranim ili decentraliziranim mrežnim sustavima, su otporni na pokušaje „rušenja“ mreže konvencionalnim metodama kao što su zabrane „rudarenja“ ili korištenja digitalnih valuta u pojedinim državama. Sve dok postoji minimalni broj validatora odnosno računalnih resursa koji bi validirali transakcije u određenoj digitalnoj transakcijskoj mreži, mreža se ne može srušiti. Iz ovih razloga problemu regulacije se mora pristupiti na globalnoj razini u okviru postojećih regulativa vezanih za transfer novca i vrijednosti. Komisija za plaćanja i tržišnu infrastrukturu prepoznaje 4 kategorije regulacije tržišta(Frebowitz, 2018: 62)::

- Informacijski utjecaj – prezentiranje rizika i opasnosti investiranja u digitalne valute, rudarenja te transakcija digitalnih valuta promoviranjem općih informacija

- Regulacija privatnih financijskih institucija - regulacija mjenjačnica digitalnih valuta predstavljaju jednu od komponenti koje je moguće regulirati. Uvođenjem AML (Anti Money Laundering) i KYC (Know Your Customer) procedura te ostalih analitičkih zahtjeva i sustava za zaštitu potrošača, centralizirane mjenjačnice su u posljednjih 10 godina značajno podigle razinu sigurnosti i kvalitete usluge.
- Prilagodba interpretacije postojeće regulacije – uvrštavanje digitalnih valuta u sve „tradicionalne“ zakonske propise
- Kreiranje šire regulacije – uvrštavanje digitalnih valuta u poseban zakon kojim bi se regulirao odnos prema digitalnim valutama na način sličan tradicionalnim transakcijskim sustavima, provođenjem AML i CTF (Counter Terrorist Financing) procedura na svim transakcijama digitalnih valuta

5.3. Primjer nadzora i regulacije tržišta digitalnih valuta u SAD-u

Kao najbolji primjer reguliranog tržišta digitalnim valutama nedvojbeno se ističu SAD. Najsnažnija svjetska ekonomija ima izrazito kompleksan sustav regulacije i povezanosti svih relevantnih financijskih i sigurnosnih državnih tijela. SAD je po pitanju uređenosti tržišta digitalnim valutama svjetski lider te se smjernice, zakoni i ostali regulativni propisi doneseni u SAD-u nerijetko „prepisuju“ u drugim državama koje tek grade svoje regulacijske okvire. Mora se istaknuti kako je taj regulativni okvir te zahtjevi koji se nameću pružateljima i korisnicima financijskih usluga u sektoru digitalnih valuta izrazito rigorozan te podliježe i paleti zakona koji nisu direktno vezani uz primjenu i korištenje digitalnih valuta. Najbolji primjer razmjera regulativnog pritiska u SAD-u je činjenica da je najveća mjenjačnica digitalnih valuta Binance zapravo podijeljena na dva ogranka; „Binance SAD“ koji je ovlašten pružati financijske usluge građanima SAD-a te „Binance“ koji pruža financijske usluge trgovanja digitalnim valutama ostatku Svijeta. S obzirom na poteškoće sa definiranjem digitalnih valuta, više regulatornih i sigurnosnih tijela je kreiralo vlastite dokumente sa smjernicama u vezi transakcija, investicija i vlasništva nad digitalnim valutama. Ovakav pristup bez izravnog i sveobuhvatnog regulatornog okvira rezultirao je izrazito kompleksnim hibridnim regulatornim okolišem gdje se određene smjernice primjenjuju u ovisnosti o pojedinoj situaciji. Sukladno vrsti pojedinog sigurnosnog rizika koje određena aktivnost vezana uz digitalne valute nosi, određena institucija financijskog, obavještajnog ili sigurnosnog nadzora primjenjuje vlastite regulativne i zakonske propise.

1.) Agencije za istragu

Tradicionalne agencije za istragu u SAD-u kao što je FBI predstavljaju prvu crtu obrane u vezi kriminalnih aktivnosti vezanim uz digitalne valute, kao što je korištenje blockchain infrastrukture za izvršavanje kriminalnih radnji prijevare ili trgovine nezakonitom robom. FBI je odgovoran za rušenje Silk Road-a, nezakonitog tržišta drogama na Dark Webu-u koji je kao sredstvo plaćanja koristion digitalnu valutu Bitcoin. FBI je 2013. zaplijenio više od 29,600 Bitocina te ih par mjeseci kasnije prodao na aukciji dok je protiv utemeljitelja Silk Road-a, Rossa Ulbirchta podignuta optužnica za trgovanje narkoticima te zavjeru s ciljem pranja novca. Danas FBI ima više odjela koji se bave isključivo istraživanjem kriminalnih aktivnosti s digitalnim valutama te se specijalisti koji rade u ovim odjelima nerijetko obučavaju u suradnji sa civilnim tvrtkama kao što je Binance.

2.) Pravosuđe

Jedinica MIMF (Market Integrity and Major Frauds Unit) je nacionalni lider u procesuiranju prijevara i tržišnih manipulacija koje uključuju digitalne valute. Od 2019. jedinica je podnijela optužnice za slučajeve prijevare s digitalnim valutama koji uključuju više od 2 milijarde dolara financijskih gubitaka. Tužitelji koriste analitiku podataka s blockchaina i tradicionalne tehnike provedbe zakona kako bi identificirali i procesuirali složene sheme ulaganja u digitalne valute, manipulacija cijenama i tržištem koja uključuje digitalne valute, neregistrirane mjenjačnice digitalnih valuta uključene u prijevare te sheme trgovanja povlaštenim informacijama koje utječu na tržišta digitalnih valuta. Tužitelji u Jedinici često rade paralelno s Securities and Exchange Commission SAD-a (SEC).

3.) Porezne službe

Internal Revenue Service (IRS), glavna porezna agencija u SAD-u je 2014. godine definirala digitalne valute kao što je Bitcoin kao vlasništvo koje podliježe zakonima SAD-a te je donijela je odluku kojom se bitcoin tretira kao oporeziva imovina odnosno podliježe obvezi obračuna poreza na kapitalnu dobit. Svaki entitet koji transferira, plaća ili trguje digitalnim valutama odgovoran je za prijavu kapitalne dobiti koja je stečena uslijed tih aktivnosti.

Također, istom zakonu i propisima podliježu i plaćanja za usluge ili proizvode koja se vrše u digitalnim valutama.

Iako je ta odluka štetna po držatelje, paradoksalno ona je definirala status bitcoina u SAD-u i učinila je njegovo posjedovanje nedvosmisleno legalnim. Iako zapravo nikada nije ni bio proglašen nezakonitim oblikom imovine, do te odluke njegov status bio je u takozvanom pravnom vakuumu, bez jasnih odrednica oko njegova položaja. Time je uvođenje bitcoina u zakonske i porezne okvire otvorilo put širem krugu investitora da investiraju i ostvaruju, bar formalno, oporezive prihode od trgovine. (https://informator.hr/strucni-clanci/zakonsko-reguliranje-kriptoimovine)

Nadzor nad poreznim prijavama vezanim uz digitalne valute je izrazito teško izvršiti, pogotovo ukoliko korisnik kripto valuta nije registriran na nekoj od centraliziranih mjenjačnica već koristi decentralizirane mjenjačnice i digitalne novčanike koji nisu vezani za privatne podatke korisnika. Centralizirane mjenjačnice u SAD-u su po zahtjevu dužne dostaviti izlist svih transakcija sa prikazanom dobiti za svakog korisnika te je ovakve slučajeve puno jednostavnije riješiti radi automatizirane strukture sakupljanja podataka samih mjenjačnica. Da bi se ovakav sustav prenio i na decentralizirani sektor potreban je sveobuhvatan alat kojim bi se regulirao protok novca u digitalne valute i iz istih, te povezivao stvarni identitet korisnika sa adresom digitalnog novčanika.

4.) Komisija za trgovinu robom

Commodity Futures Trading Commission (CFTC) je neovisna regulacijska organizacija odgovorna za nadzor i regulaciju tržišta robom (eng. commodity). 2014. godine CFTC je definirao digitalne valute kao robu te je samim time nadzor nad trgovinom istima stavio pod svoj autoritet. Regulativni pristup CFTC-a se sastoji od: edukacije potrošača, zakonskog autoriteta koji osigurava regulativni okvir za sprečavanje prevara i manipulacija, tržišno obavještajno djelovanje te koordinaciju između digitalnih valuta i ostalih regulatora. CFTC je poduzela niz aktivnosti vezanih uz neregulirane mjenjačnice, zabranu ilegalne trgovine te izdavanjem smjernica vezanih za digitalne valute. Pokazatelj sve veće popularnosti digitalnih valuta je vidljiv i kroz certifikaciju dva velika svjetska tržišta, Chicago Mercantile Exchange i Chicago Board of Options Exchange, čime se dozvolila trgovina Bitcoin tokenima na ovim mjenjačnicama koje tradicionalno trguju robom (čelik, nafta, drvo itd.).

5.) Komisija za trgovinu i vrijednosne papire

Glavna misija Security and Exchange Commission (SEC) je zaštita investitora, održavanje poštenog, urednog i efikasnog tržišta te omogućavanje formiranja kapitala u trgovini vrijednosnim papirima. Najveći značaj u regulaciji tržišta digitalnim valutama SEC je pružio po pitanju regulacije prikupljanju kapitala odnosno ICO (Initial Coin Offering) – Inicijalnih ponuda tokena koje su 2017. godine, u potpuno nereguliranom tržištu po ovom pitanju, nanijele velike štete investitorima željnim brze zarade na novim projektima. Iako je SEC izdao stroge smjernice za ICO-e, organizacija tek treba pojasniti smatraju li se digitalne valute vrijednosnim papirima, što ostavlja prostora za moguće buduće intervencije SEC-a na tržištu digitalnih valuta. U službenoj izjavi za javnost iz 2017. predsjednik SEC-a Jay Clayton ističe kako je definiranje digitalnih valuta kao vrijednosnog papira stvar specifikacija i značajki pojedine digitalne valute.

6.) Ured za kontrolu stranog kapitala

Office of Foreign Assets Control (OFAC) je odjel Riznice SAD-a (US Treasury) koji je 2018. uveo nove obvezne zahtjeve prema mjenjačnicama digitalnih valuta uključujući blokade računa koje OFAC proglasi prijetnjom za SAD. Lista blokiranih računa kreirana od strane OFAC-a cilja na individualce, grupe i tvrtke koje potencijalno su kontrolirane od strane označenih država ili ne državnih organizacija kao što su terorističke organizacije i narko karteli.

7.) Financial Crimes Enforcement Network

Financial Crimes Enforcement Network (FinCEN) je također odjel Riznice SAD-a (US Treasury) i odgovoran je za upravljanje provedbom regulacije nad digitalnim valutama. Misija FinCEN-a je zaštititi financijski sustav od nezakonite upotrebe, boriti se protiv pranja novca te promicati nacionalnu sigurnost kroz prikupljanje, analizu financijskih obavještajnih informacija i strateške uporabe financijskih ovlasti.

FinCEN definira digitalne valute kao medij za razmjenu koji se u određenim slučajevima koristi kao prava valuta, no nema sve značajke prave valute jer nema status službene valute u niti jednoj državi na svijetu. Stoga se interes FinCEN-a prema digitalnim valutama zasniva na sposobnosti digitalnih valuta za iznimno brzu i efikasnu zamjenu za američke dolare i obrnuto.

5.4. Primjer regulacije tržišta digitalnih valuta u Ruskoj Federaciji

Ruska Federacija je među prvim državama u Svijetu koje pripremaju uvođenje digitalne valute izdane od strane centralne banke (CBDC) odnosno digitalnog rublja. Predsjednik Vladimir Putin je potpisao zakon o uvođenju digitalne rublje u srpnju 2023. godine te se testiranje sustava najavljuje za kolovoz iste godine. Uz fizički i elektronski oblik, digitalni rubalj će postati treći oblik valute čiju će količinu, promet i nadzor određivati i vršiti Centralna banka Rusije. Za razliku od globalnih digitalnih valuta, ovakav sustav je centraliziran iz razloga zaštite monetarne politike te održavanja financijske sigurnosti koju odražava stabilnost državne valute. Potencijalno uvođenje CBDC-a u Rusiji potaknuto je s nekoliko čimbenika. Ključna motivacija bila je modernizacija financijskog sustava i platne infrastrukture zemlje. Predviđa se da bi digitalni rubalj mogao unaprijediti učinkovitost plaćanja, smanjiti troškove transakcija i poboljšati pristup financijskim uslugama, posebno u udaljenim ili slabije pokrivenim regijama. CBDC će omogućiti i veću kontrolu i nadzor nad platnim sustavom, potencijalno smanjujući rizik od nezakonitih aktivnosti i poboljšavajući transparentnost, istodobno smanjujući anonimnost i privatnost korisnika.

Stav Ruske Federacije prema globalnim digitalnim valutama ne može se smatrati pozitivnim jer je tek 1. siječnja 2021. godine, Rusija postigla prvi značajan pravni korak s primjenom Federalnog zakona br. 259-FZ "O digitalnim financijskim imovinama, digitalnoj valuti i o izmjenama određenih zakonodavnih akata Ruske Federacije", poznatom kao Zakon o DFI (Digitalna financijska imovina). Ovaj zakon ima za cilj pružiti jasni pravni okvir vlasnicima i izdavateljima digitalne imovine u Rusiji, odražavajući globalni trend legitimizacije i regulacije digitalne imovine. Put Rusije prema regulaciji digitalnih valuta obilježila je promjena perspektive, gdje su u početku monetarne vlasti zemlje pokušavale zabraniti digitalne valute i srodnu imovinu. Međutim, prepoznavanje potencijalnih koristi za razvoj digitalne ekonomije potaknulo je promjenu pristupa. Pokretanje federalnog projekta "Pravna regulacija digitalnog okruženja" označilo je početak uspostavljanja pravnog okvira za digitalnu imovinu. Ključni korak prema reguliranju digitalne imovine u Rusiji bio je uvođenje izmjena u Građanski zakonik Ruske Federacije kako bi se uveo pojam "digitalnih prava". Ta su digitalna prava poslužila kao temelj za pravno priznanje digitalnih financijskih imovina, specifične kategorije digitalnih valuta, prema Zakonu o DFI. Zakon uvodi nove pravne koncepte poput "digitalnih prava", "digitalnih financijskih imovina" i "digitalnih valuta", a svaki od ovih pojmova predstavlja različite kategorije digitalne imovine i tretira se kao imovina

prema ruskom građanskom pravu. Ipak, digitalne valute nisu priznate kao zakonsko sredstvo plaćanja u Rusiji te je njihovo izdavanje i kretanje ograničeno na rusku informacijsku infrastrukturu. Ovaj dio zakona je svojevrsni paradoks, jer je ograničavanje prometa digitalnim valutama na isključivo rusku informacijsku infrastrukturu nemoguć radi tehničkih značajki blockchain tehnologije, te je u pravom značenju svojevrsna zabrana korištenja globalnih digitalnih valuta. Nedostatak sveobuhvatne i jednoznačne regulacije za digitalnu imovinu nije specifičan samo za Rusiju te se ovaj izazov javlja zbog izvanteritorijalne prirode digitalnih valuta i potencijalnih utjecaja regulacija na usvajanje inovativnih tehnologija poput blockchaina.

Iako ruski pravni okvir predstavlja napredak prema regulaciji digitalnih valuta, istovremeno ističe oprezan pristup monetarnih vlasti. Umjesto uspostavljanja iscrpnog i nedvosmislenog okvira, fokus se čini usmjerenim na pooštravanje regulacija kojima bi se upravljalo cirkulacijom digitalne financijske imovine, posebno digitalnih valuta.

5.5. Primjer regulacije tržišta digitalnih valuta u EU

Digitalne valute potpuno su legalne prema zakonima i propisima EU, dopuštajući državama članicama EU-a da stvaraju vlastite regulativne okvire za digitalne valute. U usporedbi sa Sjedinjenim Državama, Središnja banka EU (ECB) je smatrala da nije u odgovornosti ECB-a da zabrani ili intenzivno regulira digitalne valute. Glavni naglasak rada ECB-a vezan za digitalne valute je pristup informacijama o potencijalnim rizicima ulaganja i korištenja digitalnih valuta. Različito definiranje digitalnih valuta je ključno za stvaranje i primjenu regulativnih standarda te je tradicionalni stav ECB-a da se digitalne valute ne mogu smatrati pravim valutama, radi sljedećih razloga: digitalnim valutama nedostaje središnje tijelo (npr. centralna banka), transakcije digitalnim valutama nemaju legalnu zaštitu od strane EU te je volatilnost digitalnih valuta prevelika da bi se mogla predvidjeti ili koristiti kao oblik pouzdanog plaćanja.

Prva aktivnost na polju regulacije digitalnih valuta događa se 2013. od strane EBA (Europsko nadzorno tijelo za bankarstvo) izdavanjem upozorenja potrošačima o rizicima povezanim sa digitalnim valutama. U istom priopćenju EBA je savjetovala EU zemljama o potrebi uvođenja regulative po pitanju digitalne imovine. Nakon lokalnog maksimuma po pitanju broja korisnika i transakcija u 2013., dolazi do perioda sporijeg rasta tržišta te se

europska politička i financijska tijela tek 2016. godine ponovno oglašavaju u obliku izvješća Europskog Parlamenta, zazivajući regulaciju digitalnih valuta radi sprječavanja pranja novca i financiranja terorizma.

Tek 2017. dolazi do djelomične operacionalizacije nadzora i regulacije digitalnih valuta, uvrštavanjem mjenjačnica te digitalnih novčanika unutar AMLD4 (Anti Money Laundering Directive 4), zahtjevajući prijavu svih sumnjivih transakcija financijskim obavještajnim tijelima. Naredna iteracija navedene direktive, AMLD5, stupila je na snagu 2020. godine, pooštravajući KYC i AML standarde te propisujući obveznu registraciju tvrtkama koje posluju digitalnim valutama.

U lipnju 2022. godine je finaliziran novi zakon koji uređuje pravila nadzora nad svim aktivnostima vezanim za digitalne valute čime dolazi do zaokreta u politici EU prema istima. Novi regulacijski okvir, nazvan MiCA(Markets in Crypto-Assets Regulation), zahtijevat će od pružatelja usluga, kao što su mjenjačnice digitalnih valuta, prikupljanje i pohranjivanje informacija koje identificiraju osobe uključene u transakcije, kao i predaju informacija istražnim tijelima. MiCA koristi vlastitu definiciju "digitalne-imovine", koja glasi "digitalna reprezentacija vrijednosti ili prava koje se može prenijeti i pohraniti elektronički, korištenjem tehnologije distribuirane knjige ili slične tehnologije". Europska komisija želi zaštititi ulagače i osigurati stabilnost tržišta zahtijevajući da digitalne valute ispunjavaju iste zahtjeve transparentnosti, otkrivanja, licenciranja, usklađenosti, autorizacije i nadzora kao i drugi financijski proizvodi, dok istovremeno usklađuje pravni okvir za digitalne valute u 27 članica države Unije.

Cilj nove regulative je prevencija pranja novca i financiranja terorističkih organizacija, zaštita potrošača, definiranje odgovornosti tvrtki te sprečavanje štetnog utjecaja na okoliš. Ovim zakonom nije predviđen minimalni iznos transakcije koji je potreban za izvršavanje provjere određenog računa. Tretiranjem digitalnih valuta od strane tijela za provođenje zakona i pravosudnih tijela kao bilo koje druge imovine, iz pravne perspektive, zapljena, upravljanje i eventualna konverzija digitalnih valuta u službeni novac sada postaje puno lakši zadatak. Decentralizirana priroda digitalnih valuta ipak ostavlja prostora za mrežne transakcije (on-chain), koje neće biti obuhvaćene novim regulativama prvenstveno radi kompleksnosti sustava nadzora koji bi bio potreban za operacionalizaciju ovakvih pravila.

Iz svega navedenog vidljiv je snažan zaokret u politici EU-a i ECB-a prema digitalnim valutama kao odgovor na rastuću primjenu, popularnost i kriminalne aktivnosti vezane uz iste. Uvođenjem MiCA-e, EU polaže temelje striktnijoj regulaciji tržišta digitalnim valutama čime se približava SAD-ovom regulativnom okviru.

5.5.1 Primjer regulacije tržišta digitalnih valuta u RH

Razvoj regulativnog okvira u RH prati smjernice, upute te direktive Europske Unije, te trenutno primjenjuje zadane KYC i AML standarde. Izglasavanjem Zakona o sprječavanju pranja novca i financiranja terorizma, regulativni okvir za digitalne valute u RH je preuzeo sadržaj AMLD4 te AMLD5 direktiva EU. Tim zakonom, od 1. siječnja 2020. godine tvrtke koje se bave djelatnošću pružanja usluga razmjene virtualnih i fiducijarnih valuta i/ili pružanja skrbničke usluge novčanika koje su osnovane u Republici Hrvatskoj, postale su obveznici provedbe mjera, radnji i postupaka za sprječavanje i otkrivanje pranja novca i financiranja terorizma. U skladu s člankom 9.a sve pravne osobe i obrtnici koji namjeravaju obavljati djelatnosti povezane s virtualnom imovinom, obvezni su proći postupak registracije i upisati se u registar pružatelja usluga virtualne imovine koji vodi Hrvatska agencija za nadzor financijskih usluga (HANFA). (Hanfa, 2023.)

Ovim zakonom propisana je primjena AML i KYC procesa prilikom „unošenja“ i „iznošenja“ kapitala na blockchain. Time se iskorištava značajka pseudoanonimnosti blockchaina, te se ovim postupcima povezuje ulazna adresa korisnika sa njegovim identitetom. Daljnje transakcije su lako prative, te se prilikom „iznošenja“ kapitala također vrši isti postupak, identificirajući krajnjeg vlasnika, nakon čega se vrše iste AML provjere kao i u tradicionalnom bankarskom sustavu.

Osim HANFA-e, i Porezna Uprava, koju u ovom kontekstu također možemo promatrati kao sigurnosno financijsko tijelo kojem je jedna od zadaća sprečavanje pranja novca, provodi porezni režim definiran presudom Suda EU iz 2015. godine, koji je detaljno objašnjen u mišljenju Ministarstva financija iz 2018. godine. Stav Republike Hrvatske o digitalnim valutama, prema Zakonu o Porezu na dohodak, je takav da su digitalne valute definirane kao dohodak od kapitala te se svrstavaju u dohodak od ostale financijske imovine. Sukladno navedenom, digitalne valute ne spadaju niti pod jednu zakonom reguliranu kategoriju sredstava plaćanja te prema Zakonu o Hrvatskoj narodnoj banci (članak 21.) i Zakonu o deviznom poslovanju (članak 4.) kriptovalute ne predstavljaju novac, elektronički novac niti sredstvo plaćanja u Republici Hrvatskoj. Slijedom ovih činjenica, trgovina digitalnim valutama podliježe obračunu poreza na dohodak od kapitala (10%) uvećano za prirez. (Unija.hr, 2023.) Možemo zaključiti da prilagodba regulativnog okvira, a samim time i sigurnosnog sustava RH, uvelike prati regulativni okvir EU te da je operacionalizacija ovog okvira po pitanju nadzora i obavještajne infrastrukture još uvijek u početnoj fazi.

6. ZAKLJUČAK

Pojam sigurnosti u modernom svijetu možemo poistovjetiti sa pojmom financijska ili ekonomska sigurnost. U pozadini svih procesa koji omogućavaju funkcioniranje pojedinca, sustava i države su financije, što je i centralni motiv i sredstvo svih sigurnosnih napora. S obzirom da je ekonomska sigurnost direktno ili indirektno povezana sa svim ostalim segmentima sigurnosti, izrazito je važno postići zadovoljavajuću razinu sigurnosti transakcijskih sustava koji omogućavaju prijenos vrijednosti i nadzor novčanog toka, te čine temelj zdrave ekonomije.

Digitalne valute i blockchain tehnologija predstavljaju velik iskorak u razvoju moderne financijske infrastrukture. Napredne značajke modernih digitalnih transakcijskih sustava baziranim na blockchain tehnologiji omogućuje dosad nepojmljivu razinu skalabilnosti, sigurnosti i praktičnosti uz promjenjivu razinu anonimnosti. Činjenica da pojedine digitalne transakcijske mreže bez centralnog tijela mogu procesuirati četverostruko više transakcija u sekundi od VISA sustava, sa skoro nikakvom vjerojatnosti za pad sustava i uz minimalne troškove u realnom vremenu govori o superiornoj tehnologiji koja će u budućnosti biti neizbježan dio svjetskog financijskog sustava. Kao i svaka nova tehnologija i ova se susreće sa problemima koji proizlaze iz skoro nepostojećeg regulativnog okvira te znatno brže prilagodbe kriminalnih skupina naspram državnih sigurnosnih tijela. Nesrazmjer u financijskoj dobiti privatnog i kriminalnog sektora naspram državnih službi uvjetuje odljev stručnjaka koji su prijeko potrebni za razumijevanje nove tehnologije te kreiranje zakonskog okvira i institucionalnih alata za provedbu istih. Iz ovih razloga, svi ozbiljni rizici i nedostaci blockchain tehnologije su izašli na vidjelo u prvih nekoliko godina od pojave ove tehnologije i povezanih financijskih proizvoda. Pristup novoj tehnologiji države su prilagodile stanju vlastite ekonomije i ovlastima vlada koje su proizvod političke strukture u pojedinoj državi. Tako su države čija službena valuta, uvjetovana nestabilnom ekonomskom situacijom, ima izraženo inflatorno kretanje, izabrale tvrđi pristup novonastaloj situaciji te u potpunosti zabranile korištenje digitalnih valuta. Nužno je naglasiti kako je fundamentalni razlog ovakvog pristupa zaštita monetarne politike i stabilnosti ekonomskog sustava države za razliku od država poput SAD-a, gdje je glavni cilj regulacije kontrola tržišta, zaštita potrošača te sprečavanje financiranja terorizma i pranja novca. Usporedbom SAD kao ekstrema po pitanju regulacije digitalnih valuta te EU kao „početnika“, možemo izvesti četiri zaključka.

Prvi, da je definiranje pojma digitalnih valuta od vitalne važnosti za određivanje jurisdikcije određene institucije nad rizičnim aktivnostima te razvijanje regulativnog okvira. U SAD-u su različite institucije definirale digitalne valute na različite načine tako da su u regulativnu operacionalizaciju uključena porezna, robna, trgovinska, sigurnosna te monetarna tijela državnog aparata, čime se znatno otežava pravilno funkcioniranje tržišta digitalnih valuta. S druge strane, zaostajanje u izgradnji regulativnog okvira u EU je također uvjetovan kašnjenjem u pravilnom definiranju digitalnih valuta, radi čega su do nedavno digitalne valute bile zanemarene kao potencijalni sigurnosni rizik te isključene iz regulativnog okvira.

Drugi zaključak je nepostojanje jedinstvene regulative, nadnacionalne konvencije ili ugovora kojim bi se ujednačilo definiranje pojma digitalnih valuta i imovine, te pravni okvir po kojem bi se transakcije i vlasništvo nad istima mogli regulirati. Ovakvo stanje uvjetuje niz operativnih problema kao slaba koordinacija među sigurnosnim tijelima različitih država, neujednačene strategije, standardni operativni postupci te infrastrukture potrebne za nadzor transakcija digitalnih valuta. Iako je EU primjenom AMLD4 i AMLD5 podigla razinu nadzora i kontrole, i dalje je potreban sveobuhvatan zakonski okvir, koji bi ujednačio praksu na razini cijele EU.

Treći zaključak je kako je izgradnja stabilnog, efikasnog i nenametljivog sustava reguliranja trgovine i transakcija digitalnih valuta neizbježna ukoliko želimo postići sigurno financijsko tržište i otvoriti put širokoj primjeni blockchain tehnologije. Razmjeri nastalih financijskih šteta, povezanost terorističkih organizacija sa digitalnim valutama te pranje novca dosegli su maksimalne vrijednosti u posljednjih nekoliko godina te su i najzagriženiji protivnici regulacije prihvatili uređenje tržišta i nadzora transakcija kao jedinu opciju ka osiguravanju održivog tržišta i sigurnosti korisnika. Ipak, posezanje za prestrogom kontrolom kojom bi se pokušala nadoknaditi decentraliziranost, koja je u osnovi ovog koncepta, predstavljalo bi odraz nemirenja s pojavom opće digitalizacije svijeta.(https://informator.hr/strucni-clanci/zakonsko-reguliranje-kriptoimovine#footnote-2580-21)

Četvrti zaključak proizlazi iz arhitekture blockchain tehnologije. Trenutni alati za nadzor i regulaciju digitalnih valuta su ograničeni na vanmrežne transakcije (off-chain) te razmjenu službenih FIAT valuta za digitalne i obrnuto. Praćenje transakcija na mreži (on-chain) je u teoriji jednostavno radi značajke transparentnosti blockchaina, ali je povezivanje adresa digitalnih novčanika sa identitetom korisnika sve izazovnije radi pojave novih tehnologija koje podižu razinu anonimnosti na najveći stupanj. Upravo zato je regulativni okvir usmjeren na „uska grla“ tržišta i sustava transakcija digitalnih valuta: mjenjačnice digitalnih valuta te razmjenu FIAT valuta u digitalne i obratno. Podizanjem razine kontrole ulaska i

izlaska kapitala na tržište digitalnih valuta i primjenom važećih transakcijskih propisa, regulativna tijela kompenziraju manjak utjecaja u mrežnim transakcijama (on-chain).

Regulativni okviri država su u stalnom postupku razvoja i prilagodbe novonastalim rizicima koje predstavljaju digitalne valute. Treba istaknuti kako je ovo tržište izrazito „mlado“ te svakodnevno evoluira pružajući nove mogućnosti korisnicima, ali i kriminalnim skupinama. Ipak, smatram kako je budućnost svjetskog monetarnog sustava namijenjena digitalnim transakcijskim sustavima te kako uz pravilnu izgradnju smislenih regulativnih pravila i alata možemo stvoriti pravedniji, efikasniji i inkluzivniji transakcijski sustav.

7. LITERATURA

Knjige i članci:

1. Chaum D. (1982.), Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups
2. Haber S., Stornetta W.S. (1991.), How to Time-Stamp a Digital Document
3. Nakamoto, S. (2008.), Bitcoin: A Peer-to-Peer Electronic Cash System
4. A. Stankevicius, A. Andrulevicius T. Limba, K. Driaunys (2020.); Cryptocurrency and national security: Peculiarities of interaction
5. Maria Constantinescu,(2018.); Cryptocurrencies – National security implications
6. United States Department of Justice (2020.); Report of the attorney general's cyber digital task force
7. J.Baron, A. O'Mahony, D. Manheim,C.Dion-Schwarz (2015.); National security implications of virtual currency-examining the potential for non-state actor deployment
8. C. Dion-Schwarz, D. Manheim, P. B. Johnston (2019.); Terrorist use of cryptocurrencies- Technical and organizational barriers and future threats
9. M. Demertzis, G. B. Wolff (2018.);The economic potential and risks of crypto assets: Is a regulatory framework needed?
10. S. Dudley, T. Pond, R. Roseberry, S.Carden (2019.); Evasive maneuvers- How malign actors leverage cryptocurrency
11. E.Zamani, , Y. He, M. Phillips,(2018); On the security risks of the blockchain
12. Policy department for citizens rights and constitutional affairs of EU parlament (2018.): Virtual currencies and terrorist financing: assessing the risks and evaluating responses
13. S. Pandya, M. Mittapalli, O. Landau, S. Gulla (2019.), Cryptocurrency: adoption efforts and security challenges in different countries
14. M. Conti, S. Kumar E, C. Lal, S. Ruj (2017.) A Survey on Security and Privacy Issues of Bitcoin

Internetski izvori:

1. Wikipedia – David Chaum (2022.), https://en.wikipedia.org/wiki/David_Chaum, (pristupljeno: 25.07.2022.)
2. Decrypt (2022.), https://decrypt.co/109848/ethereum-energy-carbon-footprint-down-99-percent-merge (pristupljeno: 28.07.2022.)
3. UVNS (2020.), https://www.uvns.hr/hr/aktualnosti-i-obavijesti/nacionalno-vijece-za-kiberneticku-sigurnost-donijelo-odluku-o-uspostavi-radne-skupine-vijeca-za-implementaciju-direktive-2016-1148-nis-direktiva (pristupljeno: 28.07.2022.)
4. Investopedia (2019.), https://www.investopedia.com/terms/s/silk-road.asp (pristupljeno: 30.07.2022.)
5. Forbes (2022.), https://www.forbes.com/sites/rosemariemiller/2022/10/26/tornado-cash-sanctions-by-us-treasury-draw-outrage-suits-from-crypto-community/?sh=4a05cc70584c (pristupljeno: 30.07.2022.)
6. Coindesk (2022.), https://www.coindesk.com/learn/china-crypto-bans-a-complete-history/ (pristupljeno: 30.09.2022.)
7. FinCEN (2022.), https://www.fincen.gov/ (pristupljeno: 05.10.2022.)
8. Akingump (2022.), https://www.akingump.com/en/news-insights/eu-close-to-introducing-groundbreaking-law-to-regulate-crypto.html (pristupljeno: 20.10.2022.)
9. Hanfa (2023.), https://www.hanfa.hr/upozorenja-hanfe/virtualne-valute/# (pristupljeno: 01.08.2023.)
10. Unija (2023.), https://unija.com/hr/porezni-tretman-kriptovaluta-u-republici-hrvatskoj/ (pristupljeno: 07.08.2023.)