https://doi.org/10.38190/ope.12.2.7 *Stručni rad / Professional paper*

IDENTIFIKACIJA KOMERCIJALNE BLOCKCHAIN TEHNOLOGIJE TE IZAZOVI I OPASNOSTI PRIMJENE KROZ KONKRETNE PRIMJERE

Hrvoje Horvatić, bacc. oec
Europska poslovna škola Zagreb - EBUS
Selska cesta 119, 10110 Zagreb, Hrvatska
Tel.: 098 379 940, e-mail: hrvojeh@outlook.com

Vitomir Tafra, mag. oec
Europska poslovna škola Zagreb - EBUS
Selska cesta 119, 10110 Zagreb, Hrvatska
Tel.: 098 208 175, e-mail: vitomir.tafra@zrinski.org

SAŽETAK

Blockchain je revolucionarna tehnologija s velikim potencijalom primjene u mnogim granama industrije i integracije u svakodnevni život ljudi kao tehnologija pouzdane razmjene podataka kroz Internet svega (IoE). Razvoj blockchain tehnologije i kriptovaluta blisko su povezani i imaju zajednički izvor u Genesis bloku prvog potpuno funkcionalnog blockchaina, globalno najpoznatijeg kroz digitalnu kriptovalutu Bitcoin. No iako je blockchain tehnologija komercijalno dostupna već više od deset godina, šira javnost još uvijek površno i nedovoljno razlikuje pojmove blockchaina od imena najpoznatije kriptovalute. Istinska vrijednost i korist blockchain tehnologije vidljiva je kroz promatranje procesa digitalnog povjerenja. Kod načina na koji se započinju klasične poslovne transakcije ili ugovori, ne postoji univerzalno povjerenje svih strana koje su sudionici u transakciji. Tijekom klasičnih transakcija, desetljećima smo zato stavljali zakonom akreditirane institucije u središte takvih transakcija i dogovora. Do pojave blockchain tehnologije (koja je stvorena i zbog utjecaja velike ekonomske krize 2008.g, uzrokovane nepoštenjem i ilegalnim djelovanjima velikih svjetskih banaka, tadašnjih vladajućih političara i trgovaca nekretninama kao direktnih uzročnika krize), prava tehnološka rješenja problema nepovjerenja zapravo i nisu postojala. Ovaj članak analizira slučajeve komercijalne primjene i uporabu blockchain tehnologije, te identificira utjecaj, izazove i opasnosti blockchain tehnologije. Članak opisuje specifičnosti blockchain tehnologije, digitalnih kriptovaluta, aktualnu komercijalnu primjenu blockchain tehnologije te prepoznaje postojeće i moguće buduće probleme razvoja blockchaina kroz tehnološku transformaciju i implementaciju u IoT i IoE.

Ključne riječi: *blockchain; Bitcoin; digitalno povjerenje; kriptovalute; IoE*

1. UVOD

S pojavom Bitcoina i drugih kriptovaluta, blockchain tehnologija stvorila je veliki potencijal i promijenila način na koji komuniciramo s digitalnim svijetom (Fan, 2020). Blockchain je kontinuirano rastući lanac zapisa koji se nazivaju blokovi. Blokovi su povezani i zaštićeni pomoću kriptografije. Međutim, usvajanje blockchaina je prilično sporo zbog niza čimbenika, i unatoč brojnim prednostima blockchain tehnologije. Cilj je identificirati postojeće i moguće buduće probleme razvoja blockchaina kroz tehnološku transformaciju i implementaciju u IoT i IoE, te kritički analizirati konkretne primjere usvajanja blockchaina jer iako rast popularnosti blockchain tehnologije nudi brojne prednosti u odnosu na tradicionalne baze podataka, praktično korištenje blockchain tehnologije suočava se s mnogim izazovima. Tako na primjer, kriptoimovina trenutačno, u pojašnjenju regulatorskih i zakonodavnih institucija, ima obilježja špekulativnog ulaganja, i nije zakonodavno dovoljno dobro regulirana. Ulaganjem u kriptoimovinu (na različite načine, od kriptovaluta, crowdsharinga, digitalnih vrijednosnica pa sve do NFT-a i ostalih digitalnih vrijednosti u IoE ili Metaverzumu) (Gerard, 2021), može se izgubiti uloženo s obzirom na činjenice da kriptoimovina nema pokriće, odnosno podršku ili jamstvo središnje banke, kao ni bilo kojega legalnog zakonodavca ili javnog državnog tijela (HNB, 2021).

2. PREGLED OSNOVA BLOCKCHAIN TEHNOLOGIJE

Blockchain je engl. naziv za distribuiranu bazu podataka (u slučaju kriptovaluta blockchain možemo nazvati „glavnom knjigom“ ili „javnom knjigom“ zapisa - eng. “public ledger”) koja postoji na više računala istovremeno. Blockchain konstantno raste, unaprijed programiran, tako da mu se dodaju novi setovi (blokovi) informacija nakon odgovarajuće provjere autentičnosti i provjere od strane imenovanih sudionika u mreži. Blockchain možemo na hrvatskom jeziku opisati kao “lanac digitalnih zapisa u blokovima”, što nije toliko praktično pa se u nedostatku hrvatske složenice, kako bi se izbjegle nejasnoće u komunikaciji, koristi engleski naziv. Svaki blok sadrži vlastitu vremensku oznaku, vlastiti zapis kao i vezu s prethodnim blokom, tako da oni čine neprekinuti lanac digitalno kriptiranih informacija. Blockchain tehnologija se zasniva na ideji da se kriptirana informacija javno razmjenjuje između svih članova koji sudjeluju u blockchain sustavu.

2.1. Kratka povijest i značenje blockchaina

Prva pojava blockchain tehnologije prema široj javnosti vezana je uz pojavu digitalne valute Bitcoin koja je bazirana na blockchain tehnologiji. Bitcoin se pojavljuje s prvim objavljenim “Genesis” blokom koji je pokrenut i postavljen 03.siječnja 2009. godine od strane anonimnog razvojnog programera koji je svoje radove i ideje objavljivao pod pseudonimom Satoshi Nakamoto. Teorija o blockchain tehnologiji objavljena je 31. listopada 2008.g objavom linka (na internet stranici www.bitcoin.org) na mailing listu vezanu uz kriptografiju, na članak pod nazivom “Bitcoin: A Peer-to-Peer Electronic Cash System” (Nakamoto, 2008).

2.2. Satoshi Nakamoto

Satoshi Nakamoto je ime pod kojim je izumitelj Bitcoin protokola (koji se koristi za kripto valutu Bitcoin) 2008.g objavio članak "Bitcoin: A Peer-to-Peer Electronic Cash System". Nakamoto (ili možda više ljudi koji se kriju iz tog pseudonima) je predložio decentralizirani pristup transakcijama, koji je rezultirao stvaranjem blockchaina. Nakamoto je najzaslužniji za stvaranje decentralizirane blockchain tehnologije. S pokretanjem Bitcoin-a stvorena je potpuno nova podloga dostupnosti i digitalnog povjerenja kroz prikaz javnih knjiga i transakcija koje nije moguće korumpirati bez vidljivih tragova promjena. U tadašnjoj komunikaciji (Nakamoto je sa suradnicima komunicirao isključivo elektroničkim putem, a nedostatak njegovih osobnih detalja znači da je nemoguće otkriti njegov stvarni identitet) objavio je da je programiranje Bitcoin digitalne valute kroz blockchain tehnologiju započeo još 2007.g. Nakamoto je osobno modificirao Bitcoin software i surađivao s ostalim programerima uključenim u projekt Bitcoin preko digitalnih komunikacijskih kanala sve do 2011.g. Tada Satoshi Nakamoto prestaje s komunikacijom i do današnjeg dana nije otkriveno tko zapravo stoji iza tog pseudonima i pokretanja blockchain tehnologije.

2.3. „Genesis Block" i nastanak Bitcoina

„Genesis Block" je dobio svoj engleski naziv jer je prvi stvoreni blok u blockchainu. Kada se računanje bloka dovrši i pošalje u blockchain, svaki novi blok upućuje na prethodni blok. U slučaju Genesis bloka, međutim, ne postoji prethodni blok na koji se on treba referencirati. Budući da ne postoji prethodni blok, početni blokovi se obično trajno programiraju u kod blockchaina. Anonimni razvojni inženjer Satoshi Nakamoto, pokrenuo je sa svojim Genesis blokom 3. siječnja 2009 Bitcoin, kao prvu funkcionalnu digitalnu kripto valutu i blockchain. Posebna zanimljivost Genesis bloka je i tekstualna poruka koja je ostavljena u samom bloku a koja na engleskom glasi: „The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." To je referenca na naslov poznatih engleskih novina The Times koje su tog istog dana objavile da je tadašnji engleski premijer dozvolio centralnoj engleskoj banci da sanira i spasi privatne banke (bank bailout). Identično akcijama mnogih drugih centralnih banaka, iz raznih država, koje su sanirale i spasile propadajuće privatne banke državnim rezervama i novo štampanim zalihama fiat valuta, to sve se događa nedugo nakon globalne financijske krize i recesije 2008.g (recesije koju su svojim ilegalnim radnjama prouzročile upravo te iste privatne banke i njihovi partneri).

Poruka upućuje na veliku i neopravdanu državnu potrošnju, za koju mnogi moderni ekonomisti ali i tadašnji entuzijasti (kao budući ulagači u kriptovalute) vjeruju da dovodi do devalvacije fiat novca (poput američkog dolara ili britanske funte). Ti potezi centralnih banaka i bijes javnosti dugoročno su se pokazali pozitivnim za Bitcoin, kojeg je Satoshi pokrenuo u pravo vrijeme. Razlog leži u činjenici da Bitcoin (i ostale digitalne kriptovalute), sa svojom blockchain tehnologijom koja stvara javne i transparentne knjige svih transakcija, mnogi moderni ekonomisti smatraju jedinom pravom zaštitom od galopirajuće inflacije. Kad vrijednost dolara ili fiat valuta pada, digitalni kriptirani novac je dobra alternativna investicija jer ga inflacijom pogođene države ne mogu obezvrijediti izdajući nove količine fiat novca bez ograničenja. Genesis blok Bitcoina je bitan jer u sebi prilično jasno sadržava osnovnu inspiraciju, namjenu i motive njegovog kreatora Satoshi Naka-

mota. Jedan dio Bitcoin povjesničara ovaj blok naziva i „Zero Block“, kao referencu na jedinu pravu financijsku revoluciju novca kroz povijest modernog doba (Blockchair, 2022).

2.4. Potreba i prednosti blockchain tehnologije

Blockchain tehnologija je trenutno jedan od najsigurnijih načina za bilježenje aktivnosti i održavanje podataka svježima, uz besprijekorno održavanje transparentne evidencije o svojoj povijesti. Zapisane i potvrđene podatke, koji su zauvijek postali dio izračunatog i završenog bloka teško se može oštetiti, korumpirati, nemoguće ih je izbrisati bez promjene kompletnog blockchain lanca, a brzina dostupnosti povijesnog traga podataka, kao i aktualnog ažuriranog zapisa je značajno veća u usporedbi s dosadašnjim klasičnih načinima pohrane podataka. S obzirom na veliku ekspanziju blockchain tehnologije, nakon prvog desetljeća postojanja, ova nova tehnologija je prilično brzo predstavljena kao kritična tehnologija za budući razvoj IoE i samim time i IoT-a kao budućnosti u koju globalno ulazimo velikom brzinom. Pri tome se ne radi samo o digitalnim kripto valutama. Bitcoin, ostale digitalne kriptovalute, ili kripto imovina, samo su mali spektar blockchain tehnologije. Uz pomoć blockchain tehnologije ljudi mogu vjerovati jedni drugima i obavljati sve vrste digitalnih transakcija, zamjena, međusobnih ugovora, pohranjivati podatke, glasati, registrirati patente ili spremati bilo koju vrstu informacija u blokove koji jednom potvrđeni i stvoreni u blockchainu zauvijek ostaju spremljeni i aktivirani u svojem izvornom i (Peer to Peer) potvrđenom obliku, bez straha od moguće izmjene, promjene ili bilo kojeg načina korupcije originalnog digitalnog zapisa. Jedna od najbitnijih karakteristika blockchain tehnologije je povjerenje. Povjerenje je i najkorisniji razlog za implementaciju blockchaina u našem rastućem i digitalizirajućem IoT i IoE svijetu. Prednosti blockchain tehnologije su i transparentnost i javna dostupnost, a brzina kojom se blockchain konkretno ostvaruje je mnogo veća u odnosu prema mnogim dosadašnjim klasičnim načinima zapisivanja (kroz standardizirane, uobičajene kanale), provjere, i potvrde istinitosti digitalnih podataka.

2.4.1. Što je „Digital Trust“?

Istinska vrijednost i korisnost blockchain tehnologije vidljiva je kroz promatranje procesa digitalnog povjerenja (digital trust). Kod načina na koji se započinju klasične poslovne transakcije, ne moramo nužno vjerovati svim stranama koje su sudionici u pojedinoj transakciji. Da bi riješili taj problem povjerenja, tijekom klasičnih transakcija, desetljećima smo stavljali pouzdane i akreditirane institucije u središte tih transakcija. Kada se kupuje kuća, imamo posredovanje između te transakcije u obliku odvjetnika, bankara, agenata nekretninama, državne institucije koje jamče istinitost vlasništva u obliku katastra i gruntovnice. Sve to su klasična vrsta posrednika koji svojim akreditacijama (od strane zakonodavca) daju svoju vrstu specifičnog osiguranja o istinitosti i pouzdanosti informacija o predmetu transakcije. Svi oni rješavaju jedan određeni segment prodaje nekretnine nekom drugom, ali samo jedan dio kompletne transakcije i stavljajući se u sredinu između uključenih ili zainteresiranih strana za tu transakciju. Bilo da je to dug koji se preuzima kod prodaje kuće, stanje kuće ili ostale podatke o imovini koja je predmet transakcije. Kod kupnje ili prodaje, uvijek netko stoji usred te transakcije, jer prodavač ne vjeruje kupcu (i obratno) bez pouzdanih posrednika. Posrednici, svaki prema svojoj funkciji, provjeravaju za obje uključene strane jesu li informacije koje se međusobno šalju točne i pouzdane. Kad razmi-

slimo o praktičnoj primjeni stavljanja posrednika ispred ili bolje rečeno u sredinu svih ovih različitih segmenata jedne pojedinačne transakcije, vidimo da je klasičan način posredovanja dugotrajan, spor i vrlo skupi proces. Slični posrednici postoje u gotovo svim klasičnim transakcijama našeg društva, vezanima uz razmjenu novca, informacija i ostalih vrijednosti. Klasični, akreditirani posrednici stvaraju u digitalnom društvu i IoT zajednici problem „uskog grla" radi svojih troškova i sporosti, no najveći problem stvaraju kroz svoju nepouzdanost, mogućnost pogreške ili korupcije, što dovodi do nepovjerenja i velikih problema u realizacijama željenih transakcija.

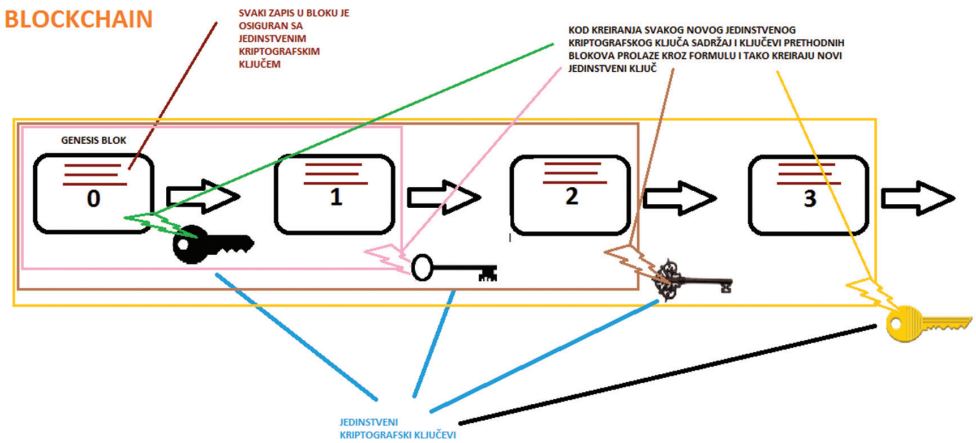
S blockchain tehnologijom i višestrukom koristi koju ta tehnologija pruža, ovaj problem konačno možemo efektno riješiti dopuštajući blockchainu (koji vrši ulogu svima pouzdanog posrednika) bez potrebe za trećom, neovisnom stranom, koja bi trebala potvrditi istinitost. blockchain tehnologija, da svojom brzinom, niskim troškovima i visoko kriptiranom sigurnošću informacija ponudi potrebno digitalno povjerenje (digital trust,eng.) svim sudionicima transakcija. Blockchain tehnologija kroz svoje procese omogućava sudionicima transakcije da vide istu verziju ili isti status transakcije i informacija u isto vrijeme, te da su sve informacije, jednake i nepromjenjivo zapisane u tim zauvijek povezanim blokovima informacija (digitalnoj javnoj knjizi). (Fan, 2020)

2.4.2. Kako blockchain mreža održava sigurnost?

Blockchain je kontinuirano rastući lanac zapisa koji se nazivaju blokovi. Blokovi su povezani i zaštićeni pomoću kriptografije. Pošto se radi o decentraliziranom sustavu, blockchain lanac održava više sudionika na mreži (računala) i oni su odgovorni za osiguranje točnosti podataka. Kod tradicionalnih transakcija, nepoznati posrednici i nepoznati sudionici (računala) nemaju povjerenje sudionika o točnosti informacija. Za razliku od tradicionalnih institucija (banke, državne institucije i slični ovlašteni posrednici) odgovornih za vođenje i kontrolu takvih zapisa, blockchain je dizajniran da bude nepromjenjiv. Svaki zapis (kao dio jedinstvenog bloka) koji je unesen u blockchainu osiguran je jedinstvenim kriptografskim ključem. Taj ključ je, zbog svoje kriptografske kompleksnosti (SHA256), s današnjom komercijalnom računalskom tehnologijom praktički nemoguće hakirati. Za takvu hakersku operaciju bila bi potrebna ogromna snaga (za sad još nepostojećih) superračunala, a potrebno vrijeme za takvo dekodiranje trajalo bi tisućama godina što je praktički besmisleno. (Makoto Yano, 2020)

Kada se novi zapis upiše u aktualni blok, sve iz prethodnog zapisa, uključujući njegov sadržaj i njegov ključ, šalju se kroz formulu za generiranje ključa drugog zapisa. Ova interakcija stvara ovisnost među blokovima. Kada se kreira sadržaj trećeg zapisa, ključevi prva dva zapisa stave se u formulu za uspostavljanje trećeg ključa. Ova ovisnost među zapisima povezuje sve zapise zajedno. Zatim se isti postupak ponavlja sve dok se blok ne napuni (kod Bitcoin blockchaina svaki blok sadrži maksimalno 1 MB podataka što je dovoljno za otprilike 4000 transakcija, a novi blok se dodaje u blockchain otprilike svakih 10 min.). Na ovaj način, svaki novi kreirani zapis čini izmjenu povijesti blockchaina sve složenijom, a blockchain je otvorena i transparentna "knjiga" (public ledger, eng.), te sva računala uključena u mrežu može istovremeno provjeriti da li je povijest blokova točna kroz osvrt na prethodne blokove. (Kapu, 2020)

Slika 1. Blockchain je set protokola i kriptografskih metoda



Izvor: *rad autora*

2.5. Decentralizacija i modeli upravljanja temeljeni na blokovima

Društvena decentralizacija koju omogućuje blockchain potencijalno može redistribuirati i ponovno demokratizirati obrasce ljudskog sudjelovanja i suradnje. Blockchain ne kontrolira središnje tijelo, već mreža sudionika, koji sami uspostavljaju pravila za sudjelovanje i mogu razvijati sustav prema konsenzusu; to ih čini otpornima na cenzuru i strukturalno elastičnijim od većine drugih mehanizama donošenja odluka (za veće skupine ljudi). Decentralizacija je proces disperzije funkcija i moći sa središnje lokacije ili središnje vlasti. U decentraliziranoj arhitekturi teško je razlučiti određeno središte. World Wide Webje izvorno razvijen kao decentralizirana platforma.

2.5.1. Što su posrednici (intermediaries) i koji su rizici povezani s kriptoimovinom?

Odabir pravog distribucijskog kanala ključan je za uspjeh. Kod angažiranja posrednika uvijek treba biti svjesni postojećih implikacija. Posrednik djeluje kao povjerljiva poveznica s potrebnim znanjem, sposobnošću i sigurnošću provedbe. Blockchain ima veliki potencijal reinvencije klasičnih odnosa, razmjene informacija i transakcija koje su se do pojavljivanja ove tehnologije odvijale preko posrednika. Te operacije se između ostaloga posebno odnose na financije, bankarstvo, povjerljivo kontaktiranje, veleprodaju i maloprodaju.

Posrednici su obično angažirani jer pružaju sigurnosnu i logističku podršku te tako osiguravaju nesmetanu i učinkovitu distribuciju robe, informacija ili novca. Prije blockchaina, kupnja i prodaja zahtijevala je posrednika, banku ili brokera koji su čuvali financijske podatke svojih klijenata na svojim računalima. Kada prenosite sredstva ili kupujete, bankar se povezuje sa sustavom banke kako bi zabilježio promjenu. Blockchain tehnologija zamjenjuje ovaj središnji sustav decentraliziranom knjigom ulančanih blokova zapisa. Svaki zapis je povezan s onim prije i onim nakon njega, dajući sljedivu povijest svake transakcije. Nijedan zapis ne može se izbrisati niti se postojeći zapisi mogu mijenjati, pa prema tome u većini slučajeva blockchain tehnologija može zamijeniti klasične posrednike na kvalitetan,

brz, siguran i financijski mnogo isplativiji način. Sposobnost blockchaina da ukloni posrednika znači da može podržavati „pametne ugovore“ s uvjetnim klauzulama programiranim u blockchainu. To čini ugovor samoprovedivim, prijenosom sredstava ili ostalih informatičkih vrijednosti samo kada su ispunjeni uvjeti.

No, kriptoimovina trenutačno, u pojašnjenju regulatorskih i zakonodavnih institucija, ima obilježja špekulativnog ulaganja i nije zakonodavno dovoljno dobro regulirana. Ulaganjem u kriptoimovinu (na različite načine, od kriptovaluta, crowdsharinga, digitalnih vrijednosnica pa sve do NFT-a i ostalih digitalnih vrijednosti u IoE ili Metaverzumu) može se izgubiti uloženo s obzirom na činjenice da kriptoimovina nema pokriće, odnosno podršku ili jamstvo središnje banke, kao ni bilo kojega legalnog zakonodavca ili javnog državnog tijela. Uloženi iznosi ili ostale vrijednosti nisu osigurane, nisu u sustavu zaštite potrošača, kao npr. sustav osiguranja depozita (bankovni depozit osiguran do iznosa od 100.000 eura) i nije u sustavu zaštite ulagatelja (u Republici Hrvatskoj) te ne postoje nadležne institucije. (HNB, 2021) Prema tome, u svim svjetskim državama (čak niti u maloj južnoameričkoj državi El Salvadoru, koji je 2021.g neuspješno političkom intervencijom svojeg predsjednika pokušao implementirati Bitcoin u svoju zakonsku regulativu, čime je poremetio svoj kompletni financijski sustav i državu doveo do mogućeg bankrota niti godinu dana kasnije) još uvijek ne postoje posebne pravne zaštite glede gubitaka uzrokovanih digitalnim blockchain financijskim transakcijama ili ulaganjem u bilo kakvu kriptoimovinu u IoE. (Gerard, 2021) Kriptoimovina označuje elektroničke kriptografske zapise čije se kopije distribuiraju, pohranjuju i potvrđuju decentralizirano. Takvi zapisi, sami po sebi, nemaju vrijednost. Njihova je vrijednost određena ponudom i potražnjom u koju su istodobno ugrađena očekivanja glede porasta vrijednosti te zarade u razlici između kupovne i prodajne cijene. Upotreba kriptoimovine kao novca–u platne svrhe–gotovo je nepostojeća. (HNB, 2021)

Bez obzira na trenutno nepostojeću zakonodavnu regulaciju blockchain digitalnih kriptovaluta i kriptovrijednosti, porezni sustavi (u većini država razvijenog svijeta) uredno iskazuju, propisuju i objavljuju uredbe za oporezivanje dobitaka od kriptovaluta i ostale kriptoimovine. Kriptovalute nisu priznate kao novac, ali ako ste plaćeni u digitalnoj kriptovaluti ili obavljate bilo kakvu trgovinu ili razmjenu vrijednosti kroz blockchain digitalnu kriptoimovinu, države kroz svoj porezni sustav žele svoj dio (i taj dio iskazuju u svojim fiat valutama), što je kontradiktorno i teško pravno objašnjivo.

2.5.2.Modeli upravljanja temeljeni na blokovima

Iako su razvojni programeri prvenstveno razvili blockchain tehnologiju za pokretanje Bitcoina, blockchain infrastruktura uskoro može upravljati mnogim drugim vrstama prijenosa informacija, pružajući više usluga kroz model upravljanja temeljen na blokovima.

Tehnologije podržane blockchainom mogu potencijalno olakšati decentraliziranu koordinaciju i usklađivanje ljudskih poticaja na razini koju su prije mogle samo strukture zapovijedanja i piramidalne kontrole. Potencijalno različite primjene blockchain tehnologije daleko nadilaze financijska i poslovna ili korporacijska rješenja, iako je razumno očekivati da će početni val interesa i ulaganja iz tih sektora stvoriti veći zamah razvoja.. Daleko izvan opsega kriptovaluta, u tijeku je mnoštvo fascinantnih peer-to-peer projekata koji, upravljanjem temeljenim na blokovima (blockchainom), eksperimentiraju s novim kreativ-

nim modelima, stavljajući metapodatke, intelektualno vlasništvo, objavljivanje, provjeru činjenica i još mnogo toga u digitalne sustave. (Anderson, 2019)

2.5.3. Privatni ključevi (Private Keys)

Privatni ključ, kao što ime sugerira, je nasumično generirani broj koji se drži u tajnosti i kojeg privatno čuvaju korisnici. Privatni ključevi moraju biti zaštićeni i ne smije biti neovlaštenog pristupa tom ključu. U suprotnom, cijela shema kriptografije s javnim ključem je ugrožena, budući da je to ključ koji se koristi za dešifriranje poruka. Privatni ključevi mogu biti različitih duljina,ovisno o vrsti i klasi korištenih algoritama. Na primjer, u RSA, tipično, koristi se ključ 1024 bita ili 2048 bita. Veličina ključa od 1024 bita više se ne smatra sigurnom, preporučuje se veličina ključa od 2048 bita. (Bashir, 2020)

2.5.4. Javni ključevi (Public Keys)

Javni ključ je slobodno dostupan i objavljuje ga vlasnik privatnog ključa. Svatko tko zatim želi poslati izdavaču javnog ključa šifriranu poruku, to može učiniti šifriranjem poruke koja koristi objavljeni javni ključ, i slanjem te poruke vlasniku privatnog ključa. Nitko drugi ne može dešifrirati poruku, jer se odgovarajući privatni ključ čuva na sigurnom mjestu od strane izabranog primatelja. Nakon što primi poruku šifriranu javnim ključem, primatelj može dekriptirati poruku pomoću privatnog ključa. Međutim, postoji nekoliko zabrinutosti u vezi s javnim ključevima koje uključuju autentičnost i identifikaciju izdavača javnih ključeva. (Bashir, 2020)

2.5.5. Primjer simetrične i asimetrične enkripcije

Enkripcija je proces kodiranja poruke. Sadržaj takve kodirane poruke mogu pogledati samo odabrane osobe (kojima je poruka i namijenjena). Postoje dvije vrste enkripcije, simetrična i asimetrična enkripcija. Na primjeru simetrične enkripcije možemo shvatiti zašto je stvorena asimetrična enkripcija. Osoba A ima osjetljiv dokument koji želi podijeliti s osobom B. Osoba A koristi program za enkripciju za zaštitu tog dokumenta.

Dokument ima ugrađenu lozinku (šifru), koju je osoba A odabrala. Osoba A zatim šalje dokument do osobe B. Međutim, osoba B ne može otvoriti ovaj dokument jer ne zna šifru koju je osoba A upotrijebila za šifriranje dokumenta, pa prema tome osoba B nema ključ za otvaranje te poruke (brave). Sada dolazimo do pravog problema simetrične enkripcije. Kako da osoba A sigurno podijelili svoju šifru s osobom B. Slanje putem e-pošte je riskantno jer treće osobe mogu pronaći zaporku i upotrijebiti je za dešifriranje bilo koje poruke između osobe A i osobe B. To je problem kojeg rješavamo s asimetričnom enkripcijom. Problem je usporediv s poštanskim sandučićem na ulici. Poštanski sandučić je dostupan i izložen svakome tko zna njegovu točnu lokaciju (adresu). Možemo zaključiti da je lokacija sandučića potpuno javna. Svatko tko zna adresu može otići do sandučića i ubaciti pismo (svatko može poslati poruku ili dokument). Međutim, uz pomoć asimetrične enkripcije samo vlasnik poštanskog sandučića ima ključ za njegovo otvaranje i čitanje poruka. Korištenjem asimetrične enkripcije i osoba A i osoba B moraju generirati par ključeva na svojim računalima. Siguran način za tu radnju je korištenje algoritma. Jedan od najčešćih

je RSA algoritam. Ovaj algoritam generira javni i privatni ključ koji su međusobno matematički povezani. Javni ključevi mogu se koristiti za šifriranje podataka, ali samo odgovarajući privatni ključ može se koristiti za dešifriranje tih podataka. Iako su ključevi međusobno povezani, ne mogu se izvesti (ili otkriti) jedan iz drugog. Drugim riječima, ako znamo nečiji javni ključ, iz njega ne možemo otkriti njegov privatni ključ. Na primjeru poštanskog sandučića, javni ključ je adresa poštanskog sandučića. Adresa je podatak kojeg svatko smije znati, no vlasnik sandučića jedini ima privatni ključ koji je potreban za otvaranje tog sandučića. Osoba A i osoba B mogu tako, koristeći asimetričnu enkripciju, osigurati sigurnu međusobnu komunikaciju. Proces započinje razmjenom svojih javnih ključeva. Osoba B šalje svoj javni ključ osobi A i a osoba A šalje svoj javni ključ osobi B. Sada osoba A može poslati svoj osjetljivi dokument. Osoba A uzima dokument i šifrira ga s javnim ključem osobe B. Zatim šalje datoteku osobi B, koja koristi svoj privatni ključ da otključa taj dokument. Budući da koriste simetričnu enkripciju, samo osoba B može dešifrirati poruku. Niti osoba A ne može dešifrirati poruku jer ona nema privatni ključ osobe B. Snaga i sigurnost asimetrične enkripcije oslanja se na osobu A i osobu B i njihove mogućnosti i sposobnosti da svoje privatne ključeve dobro zaštite i sačuvaju tajnima. Kad bi napadač ukrao privatni ključ osobe A, s njim može dešifrirati sve poruke, koje su namijenjene osobi A. Međutim, napadač ne može dešifrirati poruke koje je osoba A poslala osobi B jer je za to potreban privatni ključ osobe B. Asimetrična enkripcija koristi se u slučajevima gdje je sigurnost sadržaja izuzetno važna.

2.6. Problem, predmet i ciljevi istraživanja te istraživačka pitanja

Problem istraživanja je nedovoljno razumijevanje stvarnog utjecaja, izazova i mogućih opasnosti od blockchain tehnologije kao potencijalnog sredstva za transformaciju struktura u IoE. Predmet istraživanja su konkretna primjena i identificirani limiti postojeće blockchain tehnologije. Objekt istraživanja su kriptovalute, postojeće kompanije, poduzeća, startupovi, razvojni laboratoriji te ostala udruženja koja su implementirala blockchain tehnologiju u svoje postojanje i poslovanje.

Glavni cilj istraživanja bio je utvrditi trenutno stanje, utjecaj i izazove komercijalne primjene Blockchain tehnologije. Pomoćni ciljevi istraživanja (P. C. I.) su:

P.C.I.1: Pojasniti osnovnu povijest i razvoj Blockchain tehnologije.

P.C.I.2: Utvrditi osnovne karakteristike najpopularnijih digitalnih kriptovaluta.

P.C.I.3: Raspraviti o sigurnosti Blockchain tehnologije, objasniti prednosti, nedostatke i konkretne opasnosti kod primjene Blockchain tehnologije.

P.C.I.4: Obraditi osnovni marketinški aspekt djelatnosti koje su svoje poslovanje transformirale na korištenju Blockchain tehnologije.

Istraživačka pitanja (I. P.) su:

I. P. 1.: Koje su temeljne karakteristike Blockchain tehnologije?

I. P. 2.: Kako razvoj Blockchain tehnologije utječe na kriptovalute?

I. P. 3.: Osim kriptovaluta, u kojim područjima IoE je konkretno primijenjena Blockchain tehnologija?

I. P. 4.: Kakva je sigurnost Blockchain tehnologije za korisnike?

I. P. 5.: Koje su moguće opasnosti od primjene i daljnjeg razvoja Blockchain tehnologije?

3. METODE ISTRAŽIVANJE

U ovom kvalitativnom istraživanju podaci su prikupljeni iz primarnih i sekundarnih (dodatnih) izvora podataka. Podaci iz primarnih izvora prikupili su se metodom anketiranja. Populacija za anketiranje su članovi poslovne i akademske zajednice vezani uz blockchain tehnologiju, a veličina uzorka je 60 (N=60) ispitanika. Uzorak čine razvojni inženjeri, programeri i ostali profesionalci iz IT sektora te studenti informatike, elektrotehnike i multimedije, a provedena je kod zaposlenika i vanjskih suradnika poduzeća TechWarn Media d.o.o. i Area invest d.o.o. iz Varaždina, Inceptum d.o.o. iz Zagreba, IT sektora ZABA banke te studenata i profesora Fakulteta organizacije i informatike iz Varaždina, Fakulteta elektrotehnike i računarstva iz Zagreba i studija multimedije na Sveučilištu Sjever u Varaždinu.

Instrumenti i postupak prikupljanja podataka

Istraživanje je provedeno Anketom - anketnih upitnika u online okruženju (e-anketa). Anketa-anketni upitnici poslani su na 125 e-mail adresa od čega je odgovorilo njih 60. Istraživanje je trajalo 40 dana od dana poslane ankete.

Analiza podataka

Analiza prikupljenih podataka iz primarnih izvora obrađena je deskriptivnom statistikom Podaci iz sekundarnih izvora obrađene su baze znanstvenih podataka u ScienceDirect (www.sciencedirect.com, 2022) te The ACM Digital Library - digitalna knjižnica Association for Computing Machinery, (dl.acm.org, 2022).

4. REZULTATI ISTRAŽIVANJA I RASPRAVA

Rezultati istraživanja prezentirani su deskriptivnom statistikom u grafičkom obliku na uzorku N-60. Također, provedena je evaluacija, rasprava i interpretacija rezultata istraživanja.

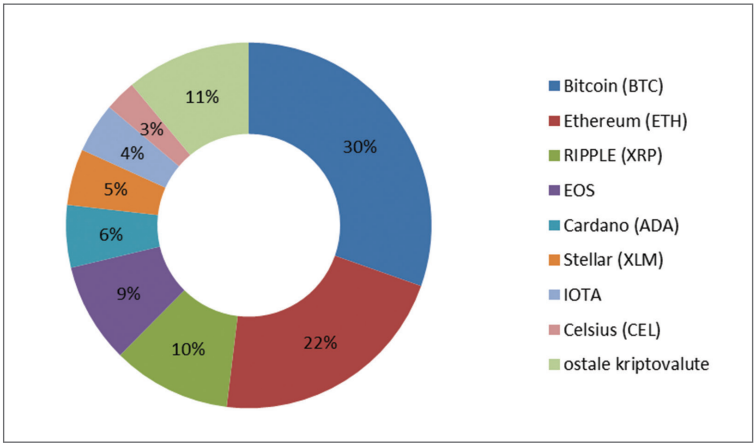
4.1 Rezultati istraživanja

U prezentaciji rezultata istraživanja navesti ćemo samo bitne odgovore iz ankete, a u obradi i analizi istraživanja uzeti su u obzir svi odgovori iz ankete.

Na uvodna pitanja o pojmu i osnovnim karakteristikama blockchain tehnologije upoznato je 93% ispitanika, dok 7% ispitanika nije upoznato s blockchainom što nam je potvrdilo reprezentativnost uzorka obzirom na poznavanje sadržaja područja istraživanja.

Također na pitanje: Koje postojeće kriptovalute želite izdvojiti kao najznačajnije u 2022 godini? sudionici ankete naveli su da su to a) Bitcoin (BTC) - 91%, b) Ethereum (ETH) - 65% dok je 83% ispitanika navodilo još sljedeće kriptovalute Ripple (XRP), EOS 1, Cardano (ADA), Stellar (XLM), IOTA i Celsius. Preostale kriptovalute, navedene su u manje od 5% ispitanika, što govori o relevantnosti odgovora ispitanika

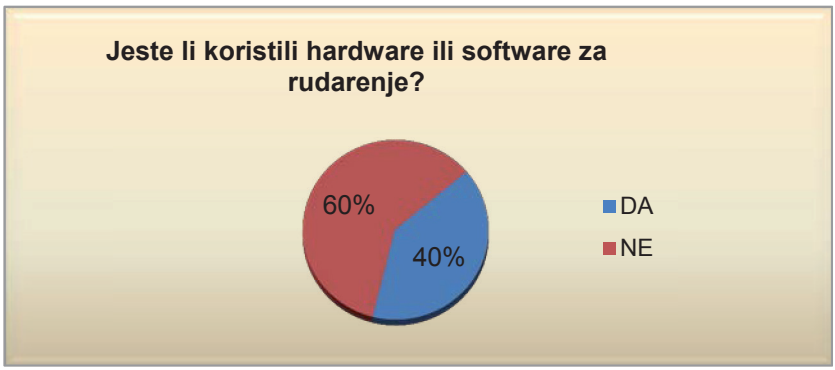
Grafikon 1. Najznačajnije kriptovalute u 2022.godini po izboru sudionika ankete



Izvor: *Izrada autora prema provedenoj anketi*

Po rezultatima ankete najznačajnije kriptovalute u 2022.g su Bitcoin s 30%, Ethereum s 22%, Ripple s 10%, EOS s 9%, Cardano sa 6%, Stellar s 5%, IOTA s 4%, Celsius s 3% odgovora. Ostale kriptovalute dobile su ukupno 11% odgovora.

Grafikon 2. Postotak anketiranih koji su „rudarili" kriptovalute



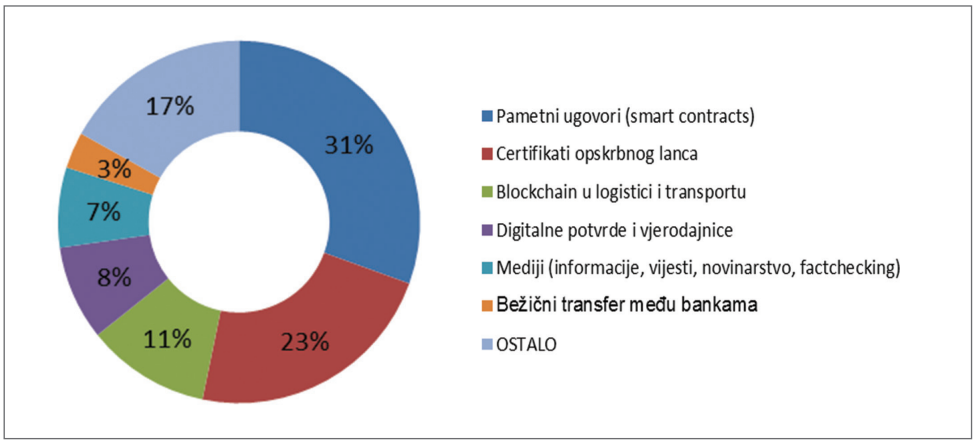
Izvor: *Izrada autora prema provedenoj anketi*

Na pitanje: Jeste li koristili hardware ili software za „rudarenje" (mining, eng.) i stvaranje vlastitih količina kriptovalute? 40% ispitanika je izjavilo da je „rudarilo", dok 60% ispitanika nije na ovaj način stvaralo vlastite količine kriptovaluta.

Na pitanje „Osim digitalnih kriptovaluta, na koji način ste konkretno koristili ili primijenili blockchain tehnologiju u profesionalnom, akademskom ili ostalim područjima primjene?" anketirani sudionici su odgovorili na sljedeći način: a) pametni ugovori (smart contracts) 78%, b) certifikati opskrbnog lanca 58%, c) blockchain u logistici i transportu 28%, d) digitalne potvrde i vjerodajnice 21%, e) mediji (informacije, vijesti, novinarstvo, fact check)

18%, dok je 43% ispitanika navelo i ostala područja konkretne primjene blockchain tehnologije, no ta područja primjene navedena su u 3 identična odgovora (<5% ispitanika).

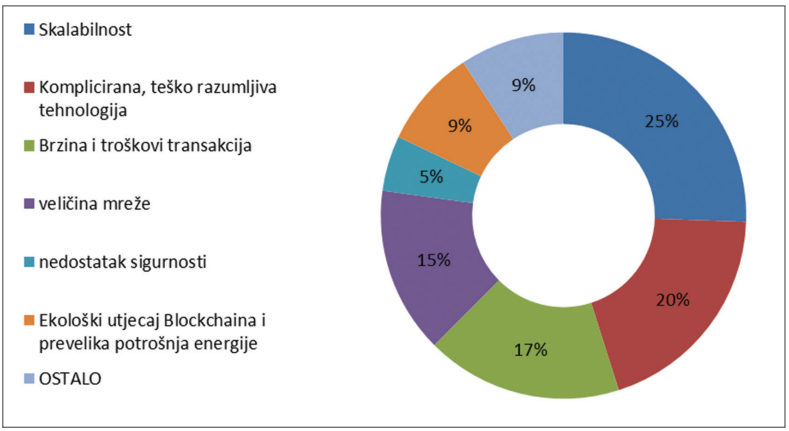
Grafikon 3. Identificirana komercijalna primjena blockchain tehnologije u profesionalnom, akademskom ili ostalim područjima s izuzećem kriptovaluta



Izvor: *Izrada autora prema provedenoj anketi*

U anketnom pitanju za identifikaciju konkretnog korištenja ili primijene blockchain tehnologije u profesionalnom, akademskom ili ostalim područjima, najviše odgovora dobilo e područje pametnih ugovora - 31%. Certifikati opskrbnog lanca čine 23%, blockchain u logistici i transportu 11%, digitalne potvrde i vjerodajnice 8%, mediji 7%, bežični transfer među bankama 3% odgovora. Ostala područja ukupno čine 17% odgovora.

Grafikon 4. identificirani nedostaci, ograničenja i potencijalne opasnosti Blockchain tehnologije



Izvor: *Izrada autora prema provedenoj anketi*

U anketnom pitanju vezanom za identifikaciju nedostataka, ograničenja i potencijalnih opasnosti blockchain tehnologije ispitanici su odabrali skalabilnost blockchain tehnologije kao najveći konkretni nedostatak u 25% odgovora. Veliki problem predstavlja i ograničenje blockchain tehnologije kao komplicirane i teže razumljive tehnologije u 20% odgovora, kao i brzina i troškovi transakcija kod blockchain tehnologije u 17% odgovora. Veličina blockchain mreže je odabrana kao negativna karakteristika u 15% odgovora, a loši ekološki rezultati i prevelika potrošnja energije u 9% odgovora. Nedostatak sigurnosti zabrinjava anketirane u 5% odgovora.

5. RASPRAVA O REZULTATIMA ISTRAŽIVANJA

Rezultati istraživanja ukazuju na potrebu uvođenja aktivnosti na boljoj, cjelovitoj i temeljitijoj informiranosti javnosti o prirodi i mogućnostima blockchain tehnologije i kriptovaluta kao i njihovim oblicima, sadržajima, namjeni, primjeni, ograničenjima te mogućim zabludama a u cilju zaštite od zloupotreba. Iz rezultata prva dva eliminacijska pitanja vidljivo je da je ispitanicima pojam kriptovaluta bolje poznat, i da je jasniji pojam od pojma blockchain tehnologije, u čemu možemo povući paralelu s pojavom internetskih domena („dot-com bubble“ 2000-tih) kada je medijska interakcija također većinom eksponirala samo jednu od mogućnosti novih tehnologija. Iako liste postojećih kriptovaluta danas bilježe tisuće unosa, većina tih šaroliko nazvanih kriptovaluta nema skoro nikakav značaj ili utjecaj na razvoj ili tržište kriptovaluta, jer su špekulativne naravi i u velikoj većini slučajeva beznačajan ili napušteni blockchain. Kroz zadnje desetljeće, nakon Bitcoina (kao prve, najpoznatije i najbitnije kriptovalute) pojavilo se mnogo digitalnih kriptovaluta koje su replike ili poboljšane verzije originalnog Bitcoin blockchaina ili pak kriptovalute koje koriste nove i inovativno razrađene tehnike bazirane na osnovnim idejama tehnologije. Mnoge od tih kriptovaluta više nemaju značaj. Prema izboru anketiranih evidentno je da je Bitcoin (BTC) kao prva, najstarija i najpoznatija kriptovaluta još uvijek najznačajnija kriptovaluta. Nakon BTC-a slijedi Ethereum (ETH), kao kriptovaluta u čijem blockchainu su implementirani prvi pametni ugovori, prve dApp aplikacije, koje je blockchain zaslužan za strelovit razvoj ostalih primjena blockchain tehnologije. Ostale uvrštene kriptovalute također su poznate po inovativnim i specijaliziranim svojstvima svojeg blockchaina radi kojih se posebno ističu. Temeljem provedenog istraživanja vidljivo je kako je 40% anketiranih koristilo neki od mogućih oblika „rudarenja“ (mining, eng.) za stvaranje vlastitih količina kriptovaluta, no većina anketiranih (60%) nisu na ovaj način koristili blockchain tehnologiju za stvaranje kriptoimovine. Konkretno korištenje ili primijena blockchain tehnologije u profesionalnom, akademskom ili ostalim područjima primjene, a koja nisu vezana uz kripto valute, čak se 31% ispitanika izjasnilo kako je koristilo ili primijenilo blockchain za pametne ugovore, 23% ispitanika koristilo je ili primijenilo blockchain tehnologiju za certifikate opskrbnog lanca (supply chain certificates, eng.), a 11% je koristilo ili primijenilo blockchain tehnologiju na području logistike i transporta. Od ostalih značajnijih konkretnih primjena blockchain tehnologije identificirane su digitalne potvrde i vjerodajnice u 8% odgovora, područje medija (informacija, vijesti, novinarstva i provjere činjenica) 7% odgovora, i područje bežičnog (wireless, eng.) transfera među bankama u 3% odgovora.

6. ZAKLJUČAK

Trenutno jedna od najpopularnijih tehnoloških inovacija, blockchain tehnologija dobila je veliku pozornost akademske zajednice i industrije. Ipak, većina populacije upoznata je samo s imenima eksponiranih kriptovaluta kao što su Bitcoin i Ethereum dok je pojam pozadinske blockchain tehnologije još uvijek slabo poznat i prilično nejasan izvan zainteresirane zajednice.

Ovaj članak kroz rezultate istraživanja identificira aktualno značajne kriptovalute te područja u kojima je komercijalna primjena blockchain tehnologije već započela. Različite aplikacije koje se temelje na blockchain tehnologiji rješavaju različite vrste ekonomskih problema, uključujući pohranu/dijeljenje informacija, stvaranje konsenzusa i upravljanje. Kroz provedeno istraživanje proširujemo razumijevanje o tome kako blockchain tehnologija konkretno utječe na organizacije i pojedince u IoT i IoE u Hrvatskoj. Također, članak je usmjeren na razumijevanje i poticanje daljnjih istraživanja i primjene blockchaina, ali i upozorava na opasnosti kod same primjene blockchain tehnologije ukoliko se dodatno ne informiramo o svim relevantnim elementima i sadržajima. Definirano je i nekoliko važnih pitanja vezanih uz izazove, opasnosti, nedostatke i ograničenja implementacije blockchain tehnologije kao što je problem skalabilnosti, interoperabilnosti, sigurnosti, problematične ekološke i energetske komponente ove tehnologije, i na kraju upitne univerzalnosti primjene blockchain tehnologije za sve problematične sektore. To su istraživačka područja u nastajanju i razvoju, a ovaj članak (kao skalirani dio puno opsežnijeg završnog rada) pruža osnovne smjernice za sve koji su zainteresirani za daljnje proučavanje blockchaina.

IDENTIFICATION OF COMMERCIAL BLOCKCHAIN TECHNOLOGY AND THE CHALLENGES AND DANGERS OF APPLICATION THROUGH CONCRETE EXAMPLES

Hrvoje Horvatić, BSc
European Business School Zagreb - EBUS
Selska cesta 119, 10110 Zagreb, Croatia
E-mail: hrvojeh@outlook.com

Vitomir Tafra, MSc
European Business School Zagreb - EBUS
Selska cesta 119, 10110 Zagreb, Croatia
E-mail: vitomir.tafra@zrinski.org

ABSTRACT

Blockchain is a revolutionary technology with great potential for application in many branches of industry and integration into people's daily lives as a technology of reliable data exchange through the Internet of Everything (IoE). The development of blockchain technology and cryptocurrency are closely related and have a common source in the Genesis block of the first fully functional blockchain, best known globally through the digital cryptocurrency Bitcoin. But even though blockchain technology has been commercially available for more than ten years, the average public still superficially and insufficiently distinguishes the terms blockchain from the name of the most famous cryptocurrency. The true value and benefit of blockchain technology is visible through observing the process of digital trust. In the way in which classic business transactions or contracts are initiated, there is no universal trust of all parties involved in the transaction. During classic transactions, that's why for decades we put institutions accredited by law at the center of such transactions and agreements. Until the advent of blockchain technology (which was also created due to the impact of the great economic crisis of 2008, caused by the dishonesty and illegal acts of the world's major banks, then ruling politicians and real estate dealers as the direct causes of the crisis), real technological solutions to the problem of mistrust did not actually exist. This article analyzes the commercial application and use cases of blockchain technology, and identifies the impact, challenges and dangers of blockchain technology. The article describes the specifics of blockchain technology, digital cryptocurrencies, the current commercial application of blockchain technology and recognizes existing and possible future problems of blockchain development through technological transformation and implementation in IoT and IoE.

Keywords: *blockchain; Bitcoin; digital trust; cryptocurrencies; IoE*

LITERATURA

1. 101 Blockchain. (20. February 2021). Preuzeto s https://101blockchains.com/blockchain-in-logistics/ (25. rujan 2022)
2. Bashir, I. (2020). *Mastering Blockchain* (3rd ed.). Packt Publishing.
3. Businesswire. (17. September 2019). Preuzeto s https://www.businesswire.com/news/home/20190917005340/en/Wells-Fargo-Pilot-Internal-Settlement-Service-Distributed (22. rujan 2022)
4. Cointelegraph. (05. November 2020). Preuzeto s https://cointelegraph.com/news/blockchain-in-journalism-winds-of-change-carry-media-to-new-frontiers (26. rujan 2022)
5. Desaulniers, D. (29. april 2022). Director of Blockchain and Data at the Associated Press. *Dwayne Desaulniers - Journalism on the Blockchain.* (F. News, Interviewer) Youtube.
6. DFINITY. (2022). Preuzeto s https://internetcomputer.org/what-is-the-ic (27. rujan 2022)
7. ACM DIGITAL LIBRARY (2022). Preuzeto s https://dl.acm.org/about (29. rujan 2022)
8. EDELMAN. (January 2022). Preuzeto s https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022%20Edelman%20Trust%20Barometer%20FINAL_Jan25.pdf (26. rujan 2022)
9. Hinsdale, J. (4. Svibanj 2022). Preuzeto s https://news.climate.columbia.edu/2022/05/04/cryptocurrency-energy/. (29. rujan 2022)
10. Iansiti, M. & Lakhani, K. (2017). The Truth About Blockchain. *Harvard Business Review.* Preuzeto s https://hbr.org/2017/01/the-truth-about-blockchain.
11. Khan, D. J. (2021). Systematic literature review of challenges in blockchain scalability. *Applied Sciences, 11*(20): 9372.
12. PROVENANCE. (2022). Preuzeto s *https://www.provenance.io/.* (27. rujan 2022)
13. Reuters. (26. APRIL 2007). Preuzeto s https://www.reuters.com/article/us-usa-education-mit-idUSN2631144020070426 (23. Rujan 2022)
14. Summers, A. (2022). *Understanding Blockchain and Cryptocurrencies: A Primer for Implementing and Developing Blockchain Projects.* (1st ed.) CRC Press (March 30, 2022)
15. Sun X, S. M. (2019). Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic. *Entropy, 21*(9): 887.
16. Van Rijmenam, M. & Ryan, P. (2019). *Blockchain: transforming your business and our world* (2nd ed.). New York, NY: Routledge, Abingdon, Oxon.
17. Science Direct (2022). Preuzeto s https://www.sciencedirect.com/ (29. rujan 2022)
18. Zhang, B. (26.06.2018). Preuzeto s https://www.chinamoneynetwork.com/2018/06/26/alibabas-alipay-launches-blockchain-cross-border-remittance-in-hong-kong (22. kolovoz 2022)
19. Zimwara, T. (20.10.2022). Preuzeto s https://news.bitcoin.com: https://news.bitcoin.com/bitcoin-embracing-el-salvador-presidents-re-election-declaration-slammed/ (23.10.2022)